Host Access for the Cloud

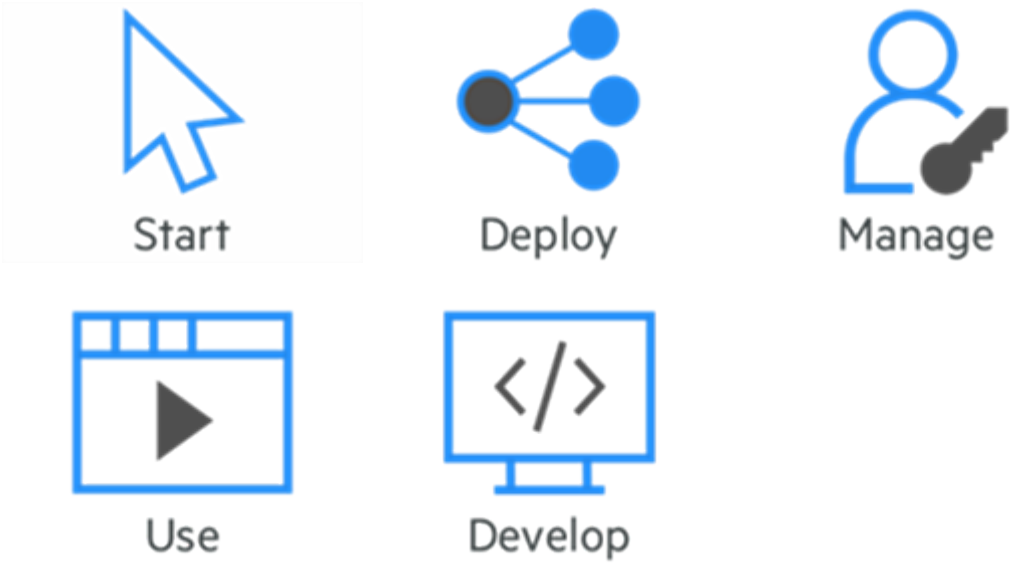
2.7.6

Table of contents

1. Willkommen bei Host Access for the Cloud

Der Host Access for the Cloud-Webclient bietet einen browserbasierten HTML5-Zugriff auf 3270-, 5250-, VT-, UTS-, ALC- und T27-Hostanwendungen. Host Access for the Cloud erfordert keine Änderungen an Ihren Desktops: Sie müssen weder Software bereitstellen noch Patches anwenden oder Konfigurationen durchführen. Sie können Benutzern plattformunabhängigen Zugriff auf alle Hostanwendungen gewähren.

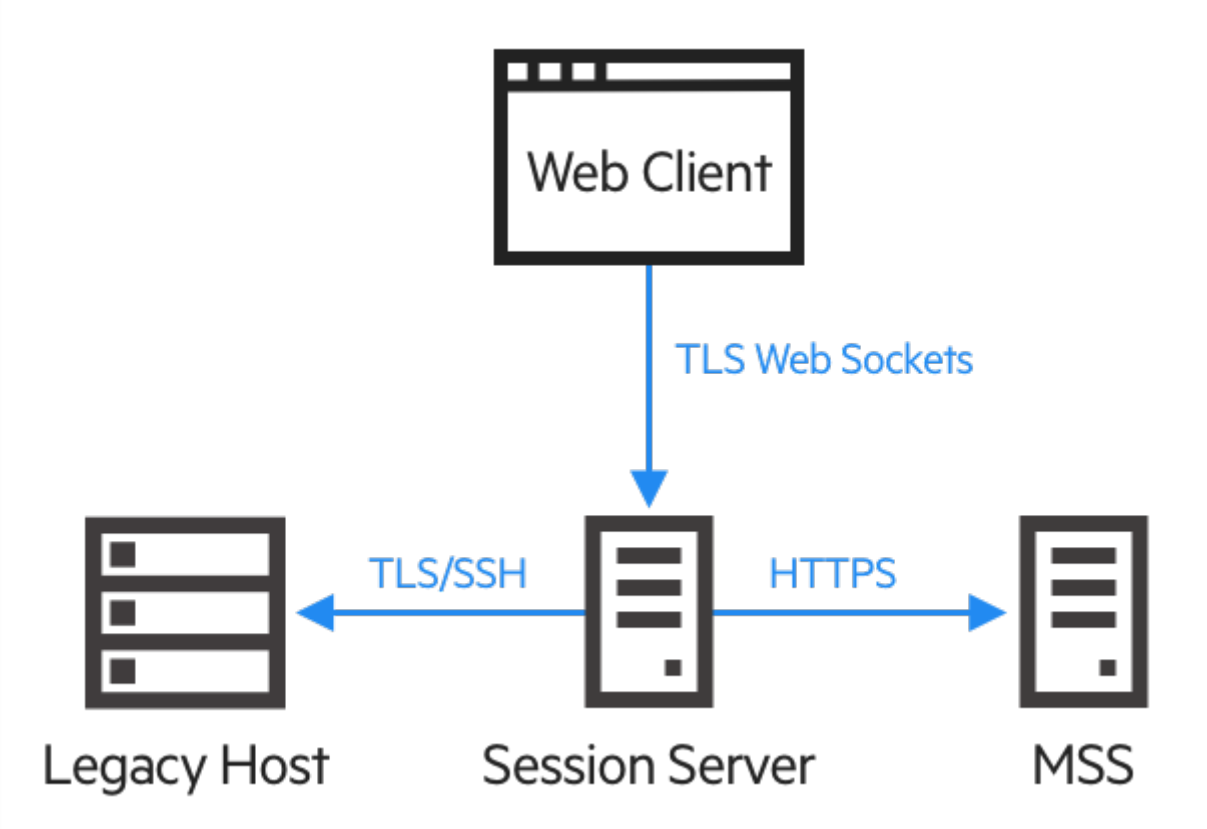
Der Webclient wird mit vollständiger Sitzungssicherung ausgeführt und verwendet TLS für die sichere Kommunikation mit Ihren Mainframe-Systemen.



2. Einführung

Host Access for the Cloud bietet eine Terminalemulation ohne Footprint (Zero-Footprint), die einen browserbasierten HTML5-Zugriff auf 3270-, 5250-, VT-, UTS-, ALC- und T27-Hostanwendungen bereitstellt, ohne dass dabei Desktopinstallationen geändert oder Java Runtime Environment-Instanzen installiert oder verwaltet werden müssen. Durch einen zentralen Verwaltungspunkt werden IT-Kosten und Zeiten für das Desktopmanagement verringert und gleichzeitig ein effizienter Hostzugriff für Endbenutzer bereitgestellt. Die Kommunikation ist durch die Verwendung von HTTPS-, TLS- und SSH-Sicherheitsmechanismen geschützt.

2.1 Funktionsweise



2.1.1 Komponenten

Machen Sie sich mit den drei Komponenten vertraut:

- Host Access Management and Security Server

  Host Access Management and Security Server (MSS) stellt eine Verwaltungskonsole bereit, bei der es sich um einen webbasierten zentralen Ausgangspunkt für das Hinzufügen, Bearbeiten und Löschen von Terminalsitzungen handelt. MSS ist Teil des umfassenderen Micro Focus-Lösungsangebots und mit anderen Micro Focus-Produkten kompatibel.

  Das Symbol MSS in dieser Dokumentation weist auf zusätzliche erforderliche Konfigurationsschritte hin, die in der MSS-Verwaltungskonsole ausgeführt werden müssen.

- Sitzungsserver

  Der Sitzungsserver ist das Modul, mit dem Endbenutzer über den Webclient und andere unterstützte Connectors sicher auf Ihren Host zugreifen können. Er bedient den Webclient und die zugehörigen Connectors am Front-End und verwaltet dann Verbindungen zum Host am Back-End, um eine ordnungsgemäße Authentifizierung und Autorisierung über MSS und eine sichere Kommunikation über TLS sicherzustellen. Mehrere Sitzungsserver können Zehntausende von Hostsitzungen bedienen und effizienten und raschen Zugriff auf Ihre Hostdaten bereitstellen.

- Webclient

  Der Webclient ist ein webbasierter Terminalemulator, über den Benutzer von einer beliebigen Plattform und anderen Orten leicht auf autorisierte Sitzungen zugreifen können.

  Im Webclient stehen Makrofunktionen, Tastaturbelegungen und Farbzuordnungen, eine Bildschirmtastatur, Funktionen zum Kopieren und Einfügen, hostgesteuerte Bildschirmaktualisierungen und Funktionen für die Dateiübertragung zur Verfügung.

2.1.2 Administrator- und Endbenutzerrollen

In der Dokumentation und im Workflow werden sowohl die Administrator- als auch die Endbenutzerrolle dargestellt. Der Administrator erstellt Sitzungen, weist diesen Sitzungen Benutzer zu und legt Benutzereinstellungen fest. Endbenutzer greifen auf die ihnen zugewiesenen Sitzungen zu, interagieren mit dem Webclient, um eine Verbindung zum Host herzustellen, und führen Aufgaben aus.

2.1.3 Unterstützung für Browser und Betriebssystem

Host Access for the Cloud ist ein 64-Bit-Produkt, das die Browser Google Chrome, Mozilla Firefox, Microsoft Internet Explorer und Microsoft Edge unterstützt. Die Verwendung von Docker-Containern ermöglicht die vertikale und horizontale Skalierung und unterstützt Cloud-basierte Technologien. Eine vollständige Liste der unterstützten Plattformen und andere Installationsanforderungen finden Sie unter „Systemanforderungen zum Evaluieren des Produkts“.

2.1.4 Sicherheitsüberlegungen

Wenn Sie Ihre Legacyhosts für Benutzer auf der anderen Seite der Unternehmens-Firewall öffnen, z. B. für Geschäftspartner, Remotebenutzer, mobile Vertriebsteams u. a., müssen Sie die Informationen vor Sicherheitsrisiken schützen. Mit Host Access for the Cloud bieten Sie allen Ihren Benutzern einen sicheren Webzugriff auf Hosts, unabhängig davon, ob diese sich ganz in Ihrer Nähe oder auf einem anderen Kontinent befinden. Host Access for the Cloud bietet zusammen mit Management and Security Server (MMS) HTTPS-Verbindungen und eine Vielzahl an Autorisierungs- und Authentifizierungsoptionen.

Host Access for the Cloud unterstützt die TLS- und SSH-Protokolle zum Schutz sensibler Daten. Um Ihre Passwörter und andere vertrauliche Daten zu schützen, verwenden Sie das HTTPS-Protokoll, welches TLS-Verschlüsselung bereitstellt.

Host Access for the Cloud kann auf sichere Weise mit dem Browser, dem Host und dem Verwaltungsserver verbunden werden. Informationen zum Sichern dieser Verbindungen finden Sie unter „Sichere Verbindungen“.

2.2 Herunterladen und Installieren von Host Access for the Cloud

2.2.1 Systemanforderungen zum Evaluieren des Produkts

Systemanforderungen für die erfolgreiche Installation und Evaluierung von Host Access for the Cloud:

- 8 GB Arbeitsspeicher
- Unterstützter Browser und unterstütztes Betriebssystem

Eine umfassende Liste der unterstützten Umgebungen finden Sie unter Mindestsystemanforderungen.

Herunterladen der Evaluierungssoftware

Wenn Sie die Software noch nicht besitzen, besuchen Sie unsere Website und füllen Sie das Formular zum Anfordern der Evaluierungsversion aus. Sie erhalten anschließend eine Email-Nachricht mit Anweisungen zum Herunterladen und Installieren einer Evaluierungsversion von Host Access for the Cloud, die 120 Tage lang gültig ist. Mit dieser Auswertungsversion können Sie Hostsitzungen öffnen und schließen und jeweils 25 aktive Hostverbindungen gleichzeitig verwalten. Die Website für die Testversion umfasst alle erforderlichen Informationen für den nächsten Schritt.

Auf der Micro Focus-Website für Downloads sind die komprimierten Dateien verfügbar, die für die Installation aller unterstützten Plattformen erforderlich sind, einschließlich Windows-Connector. Verschiedene Aktivierungsdateien ermöglichen die Aktivierung verschiedener Ausgaben/ Plattformen von Host Access for the Cloud.

2.2.2 Basisinstallation

Die folgenden Anweisungen gelten für die grundlegende Standardinstallation, d. h. alle Komponenten werden lokal installiert und verwenden die Standardports. Nach Durchführung dieser Installation können Sie die Anleitung befolgen und sich mit Host Access for the Cloud und MSS vertraut machen.

1. Laden Sie auf der Micro Focus-Website für Downloads das Installationspaket für Ihr Produkt herunter. Das Paket beinhaltet Unterstützung für alle unterstützten Plattformen.
2. Befolgen Sie die Aufforderungen im Installationsprogramm, um Host Access for the Cloud und Management and Security Server (MSS) zu installieren.

In MSS werden Aktivierungsdateien (activation.jaw) zum Aktivieren der Produktfunktionen verwendet. Das Installationsprogramm enthält die erforderliche Aktivierungsdatei. Die Aktivierung erfolgt im Rahmen des Installationsvorgangs.

> **Hinweis**
>
> Während einer Basisinstallation wird ein eigensigniertes Zertifikat verwendet, um sichere Verbindungen zu gewährleisten. Beim Wechsel zu einer Produktionsumgebung können Sie Ihre eigenen Zertifikate angeben.

Fahren Sie nun mit dem nächsten Schritt fort und machen Sie sich mithilfe der Anleitung mit Host Access for the Cloud vertraut.

2.3 Schrittweise Anleitung

Die folgende Anleitung bezieht sich auf eine standardmäßige Basisinstallation, d. h. alle Komponenten werden lokal installiert und verwenden die Standardports. Nach Durchführung dieser Installation können Sie die Schritte befolgen und sich mit Host Access for the Cloud und MSS vertraut machen.

Informationen zur Installation in Produktionsumgebungen und verschiedenen Produktionsszenarien finden Sie im Abschnitt zur Bereitstellung.

2.3.1 Auszuführende Schritte

1. Öffnen Sie die MSS-Verwaltungskonsole.
2. Neue Sitzung erstellen. Dabei wird ein neues Browserfenster geöffnet und der Bereich „Verbindung“ des Webclients angezeigt.
3. Konfigurieren Sie Einstellungen, einschließlich Verbindungs- und Benutzereinstellungsoptionen, und stellen Sie eine Verbindung her.
4. Benutzer zu Sitzungen zuweisen und Authentifizierung konfigurieren.
5. Stellen Sie den Sitzungszugriff für die Endbenutzer bereit.

Öffnen Sie die MSS-Verwaltungskonsole

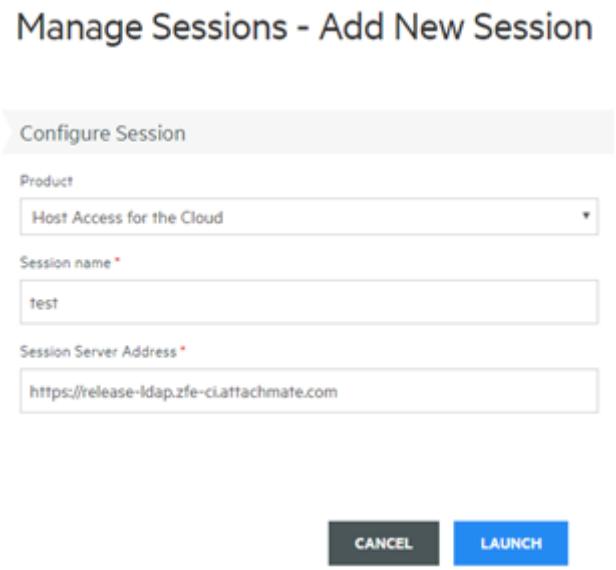
1. Klicken Sie in einer Windows-Umgebung im Startmenü unter „Micro Focus Host Access for the Cloud“ auf „Verwaltungskonsole“ oder öffnen Sie die URL für die Anmeldeseite für Administratoren in Ihrem Webbrowser. Die URL hat das folgende Format: `https://meinserver.meinefirma.com:443/adminconsole`.
2. Wenn Sie eine Verbindung über HTTPS herstellen und Ihr Server über ein selbstsigniertes Zertifikat verfügt, erhalten Sie eine Warnmeldung vom Browser über das von Ihnen erstellte Zertifikat. Hierbei handelt es sich um ein erwartetes Verhalten; Sie können das selbstsignierte Zertifikat akzeptieren oder fortfahren, um die Anmeldeseite für Administratoren zu öffnen. Nach dem Erwerb eines von einer Zertifizierungsstelle signierten Zertifikats oder dem Import des selbstsignierten Zertifikats in den Zertifikatspeicher wird diese Warnmeldung nicht mehr angezeigt.
3. Dem Administratorkonto ist ein integriertes Passwort zugewiesen: **admin**. Melden Sie sich mit diesem Passwort oder mit dem Passwort, das Sie bei der Installation von MSS angegeben haben, als Administrator an.

Neue Sitzung erstellen

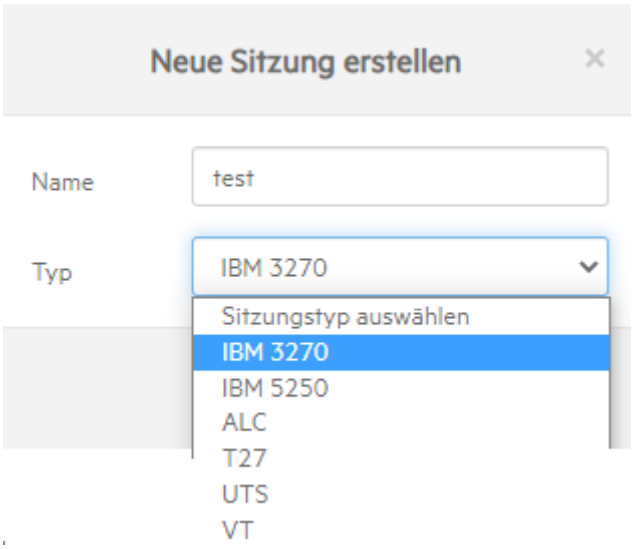
MSS Ausführliche Anweisungen finden Sie unter Add a Session (Sitzung hinzufügen) im MSS Administrator Guide (MSS-Administratorhandbuch).

Sie können Sitzungseinstellungen über den Bereich „Manage Sessions“ (Sitzungen verwalten) der Verwaltungskonsole hinzufügen und aktualisieren. Wenn Sie eine Sitzung hinzufügen, steht diese in der Liste der Sitzungen in diesem Bereich zur Verfügung.

1. Klicken Sie zum Erstellen einer neuen Sitzung im Bereich „Manage Sessions“ (Sitzungen verwalten) auf „ADD“ (Hinzufügen).



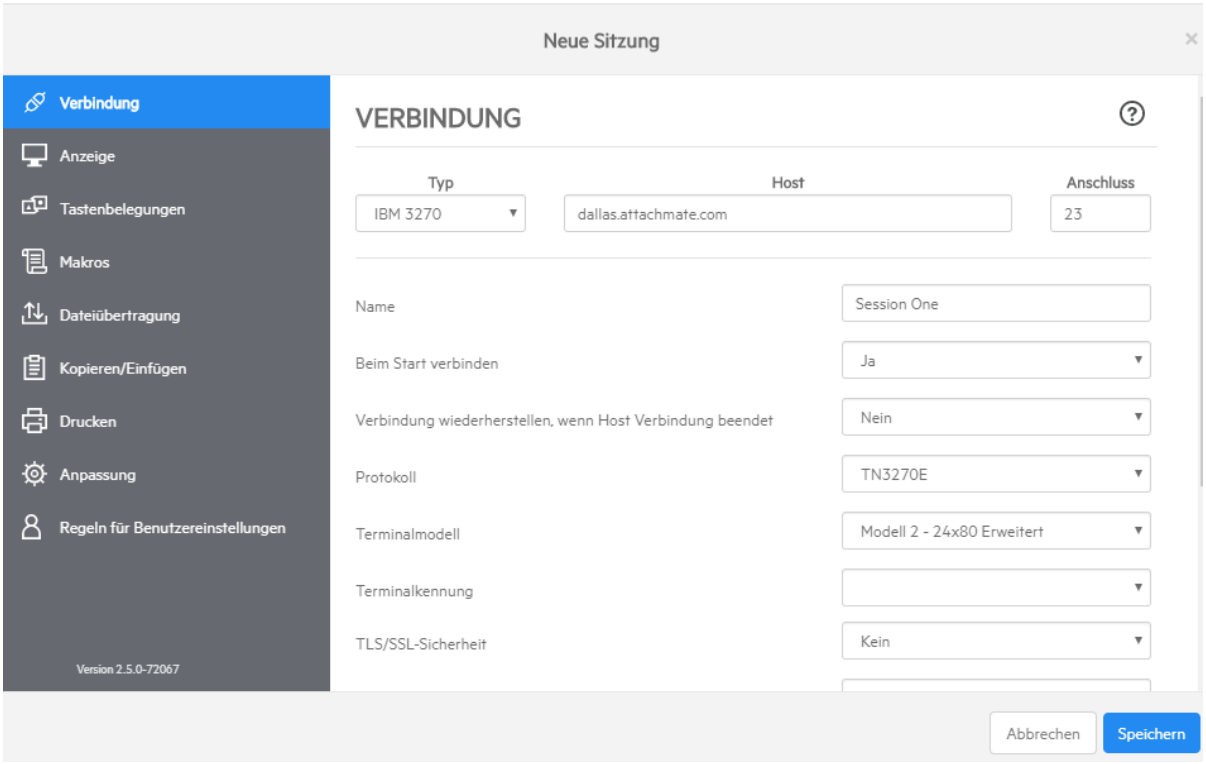
2. Sofern nicht bereits ausgewählt, wählen Sie Host Access for the Cloud als Sitzungstyp aus, geben Sie einen Sitzungsnamen ein und klicken Sie auf „Launch“ (Starten), um ein neues Browserfenster zu öffnen, in dem Sie die Sitzung für den in der Sitzungsserveradresse aufgeführten Server konfigurieren können.
3. Wählen Sie im Dialogfeld „Neue Sitzung erstellen“ den Hosttyp aus der Dropdown-Liste aus und klicken Sie auf „Weiter“.



Einstellungen konfigurieren und Verbindung herstellen

Im Browserfenster des Webclients können Sie verschiedene Einstellungen und Optionen für die Sitzung konfigurieren und eine Verbindung zum Host herstellen.

1. Geben Sie im Bereich „Verbindung“ die erforderlichen Verbindungsinformationen für die Sitzung ein, die Sie erstellen.



2. Je nach Typ der Hostverbindung können die Verbindungseinstellungen variieren. Eine genaue Beschreibung der Einstellungsoptionen für die einzelnen Hosttypen finden Sie in der Hilfe für den Webclient. Zu den Einstellungsoptionen zählt das Zuordnen von Tastenkombinationen zu

bestimmten Tasten, das Zuordnen von Hostfarben entsprechend Ihren Anforderungen und das Aufzeichnen von Sitzungsmakros.

- Tasten zuordnen

  a. Um Tasten ausgewählten Tasten zuzuordnen, öffnen Sie „Tastenbelegungen“.

  b. Drücken Sie die Taste oder Tastenkombination, die Sie zum Auslösen der ausgewählten Aktion verwenden möchten.

  c. Wählen Sie in der Dropdown-Liste „Aktion“ die Aktion aus, die der ausgewählten Tastenkombination zugeordnet werden soll. Klicken Sie auf  , um die Tastenbelegung abzuschließen. Sie können weitere Tasten hinzufügen und zuordnen.

  d. Klicken Sie auf „Speichern“, um den Vorgang abzuschließen.

- Farben für Hosts und andere Optionen ändern

  Im linken Navigationsbereich können Sie Hostfarben zuordnen, Schriftart- und Tastaturoptionen festlegen und Hotspots aktivieren, indem Sie den Bereich „Anzeige“ öffnen. Die Wahl der Farben gilt jeweils spezifisch für jede Sitzung.

- Benutzereinstellungen festlegen

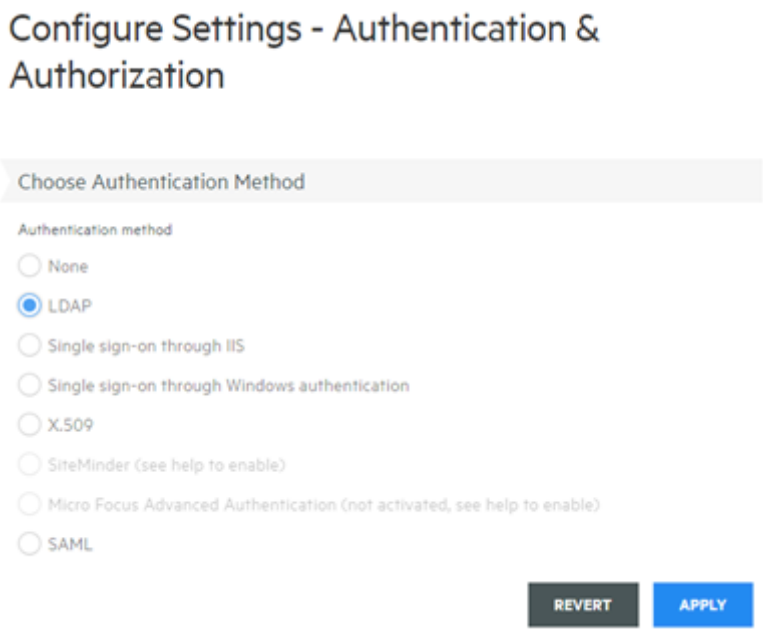
  Öffnen Sie „Regeln für Benutzereinstellungen“, um festzulegen, welche Optionen die Endbenutzer konfigurieren dürfen.

3. Klicken Sie auf „Beenden“, um zum Browserfenster der Verwaltungskonsole zurückzukehren und dort die Benutzerauthentifizierung zu konfigurieren und den Sitzungen Benutzer zuzuweisen.

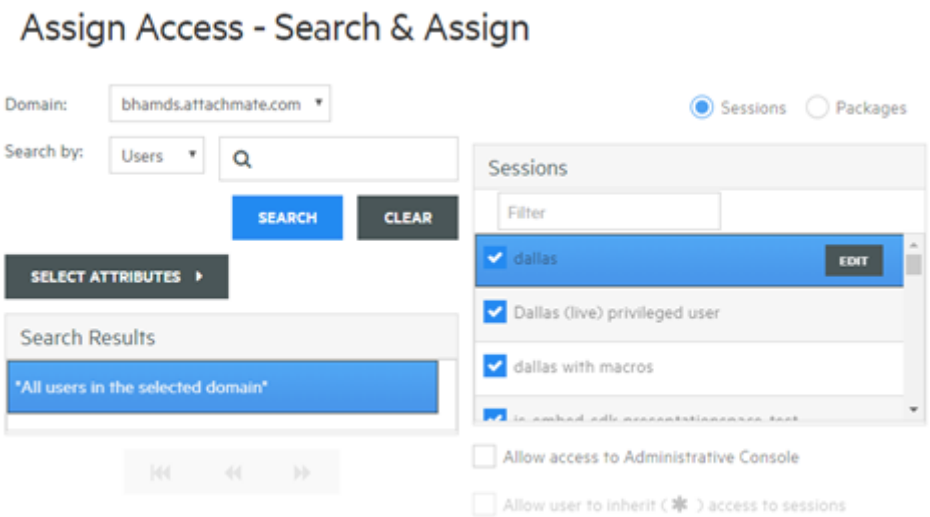
Benutzer zu Sitzungen zuweisen und Authentifizierung konfigurieren

Nach dem Erstellen der Sitzungen müssen Sie nun Benutzern Zugriff auf diese Sitzungen erteilen. Benutzer werden über die MSS-Verwaltungskonsole authentifiziert und Sitzungen zugewiesen. Ein Benutzer kann mehreren Sitzungen zugewiesen werden.

1. Die Identität eines Benutzers und die Methode für die Zuordnung von Sitzungen zu einzelnen Benutzern oder Benutzergruppen werden anhand von Authentifizierungs- und Autorisierungsmechanismen validiert. Wählen Sie im linken Navigationsbereich die Option „Configure Authentication“ (Authentifizierung konfigurieren) aus.
2. Wählen Sie eine Authentifizierungsmethode aus. Je nachdem, welche Auswahl Sie treffen, stehen Ihnen bestimmte Optionen zur Verfügung.



3. Die Beschreibung der verschiedenen Optionen finden Sie in der MSS-Dokumentation. Klicken Sie auf ?.
4. Klicken Sie auf „Apply“ (Anwenden), um den Prozess abzuschließen.
5. Öffnen Sie „Assign Access“ (Zugriff zuweisen), um Sitzungen einzelnen Benutzern oder Benutzergruppen zuzuweisen.



6. Ordnen Sie die Sitzungen den Benutzern zu, die Zugriff auf die Sitzungen haben sollen, und klicken Sie auf „Apply“ (Anwenden). Sie können auch zulassen, dass die Benutzer den Zugriff auf Sitzungen und auf die Verwaltungskonsole erben.

MSS Weitere Informationen hierzu finden Sie unter Select a method to authenticate users (Methode für die Authentifizierung von Benutzern auswählen) im MSS Administrative Guide (MSS-Administrationshandbuch).

Stellen Sie den Sitzungszugriff für die Endbenutzer bereit

Im abschließenden Schritt geben Sie eine URL zum Sitzungsserver für die Benutzer frei. Die URL ähnelt üblicherweise dem folgenden Beispiel: `https://meinServer.meineFirma.com:port`

Wenn die Benutzer auf den Sitzungsserver zugreifen, werden sie je nach Bedarf zum Anmelden aufgefordert und erhalten dann Zugriff auf die Sitzungen, die ihnen zugewiesen sind.

In komplexeren Bereitstellungen muss die URL zu einem Lastverteiler und nicht zum Sitzungsserver selbst leiten. Diese Links sind oft in Unternehmensportale oder andere proprietäre Websites eingebettet.

3. Bereitstellung

3.1 Bereitstellen von Host Access for the Cloud

Dieser Abschnitt beschreibt weiterführende Schritte, die nach der grundlegenden Einrichtung zu Evaluierungszwecken im Hinblick auf die Bereitstellung in einer Produktionsumgebung ausgeführt werden. Informationen zu einer einfachen Installation finden Sie unter Herunterladen und Installieren von Host Access for the Cloud.

- Mindestsystemanforderungen
- Info zu MSS
- Planen der Bereitstellung
- Beispielplan einer Hochverfügbarkeits-Bereitstellung
- Installation und Aufrüstung
- Ports

3.2 Mindestsystemanforderungen

Diese Plattformen *und höhere Versionen* werden von Host Access for the Cloud Version unterstützt. Die Anforderungen berücksichtigen keine anderen möglicherweise im System installierte Anwendungen oder Ressourcen.

3.2.1 Unterstützte Webbrowser

- Google Chrome 102 (empfohlen)
- Mozilla Firefox 91 (empfohlen)
- Microsoft Edge 84
- Apple iOS Safari 14

3.2.2 Sitzungsserver

- **Hardware**
  - CPU: 2 Kerne (empfohlen: 4 Kerne)
  - Verfügbarer Arbeitsspeicher: 4 GB (empfohlen: 6 GB)
- **Betriebssystem (64-Bit-Version)**
  - Windows Server 2012
  - SUSE Linux Enterprise Server (SLES) 11 SP4
  - Red Hat Enterprise Linux 7.6
  - Linux on z Systems
    - SUSE Linux Enterprise Server (SLES) 12 SP4
    - Red Hat Enterprise Linux 7.6

3.2.3 Zusätzliche Anforderungen

- Informationen zu den Systemanforderungen für MSS finden Sie im MSS Installation Guide (MSS-Installationshandbuch).
- Lastverteiler für MSS und Host Access for the Cloud müssen dauerhafte Sitzungen (sogenannte „Sticky Sessions“) und Websockets unterstützen.

3.3 Info zu MSS

Host Access Management & Security Server (MSS) sichert, verwaltet und überwacht den Zugriff der Benutzer auf Hostverbindungen. Mit MSS können Sie Sitzungen erstellen, Zählungsfunktionen einrichten und Terminalkennungen konfigurieren.

Dokumentation zu MSS:

- 12.8.6 Release Notes (Versionshinweise)
- Installation Guide (Installationshandbuch)
- Administrative Guide (Administrationshandbuch)
- Automated Sign-On for Mainframe - Administrator Guide (Administratorhandbuch für Automated Sign-On for Mainframe)

3.4 Planen der Bereitstellung

Wie viele Sitzungsserver sollten Sie bereitstellen? Wie viele MSS-Server? Welche anderen Erwägungen müssen berücksichtigt werden? Dieser Abschnitt erläutert, wie Sie die Bereitstellung der Sitzungsserver und MSS-Server optimieren.

3.4.1 Skalierung und Hochverfügbarkeit

Als ersten Schritt zur Planung der Bereitstellung müssen Sie ermitteln, wie viele Sitzungsserver und MSS-Server Sie zum Erfüllen Ihrer Anforderungen benötigen. Host Access for the Cloud kann je nach den spezifischen Anforderungen mit großer Kapazität und mit hoher Verfügbarkeit bereitgestellt werden.

Die optimale Lösung hängt von den jeweiligen Anforderungen ab. Der Abschnitt „Beispielplan einer Hochverfügbarkeits-Bereitstellung“ beschreibt ein Beispiel einer Bereitstellung, die sowohl Anforderungen in Bezug auf die Skalierbarkeit als auch auf die Hochverfügbarkeit erfüllt.

Stellen Sie sich die folgenden wesentlichen Fragen:

- Maximal wie viele Hostsitzungen werden gleichzeitig verwendet?
- Wie viele Benutzer werden das System verwenden?
- Welche Anforderungen an die Verfügbarkeit muss das System im Falle eines Fehlers in verschiedenen Systembereichen erfüllen?

3.4.2 Skalierung

Die Skalierbarkeit bezeichnet die Fähigkeit des Systems, verschieden hohe Lasten zu bewältigen. Zum Erhöhen der Kapazität kann das System vertikal hochskaliert werden, indem es auf einem leistungsfähigeren Server ausgeführt wird, oder horizontal, indem zusätzliche Server oder Knoten hinzugefügt werden.

Beide Szenarien sind mit jeweils spezifischen Kompromissen verbunden:

- Das **vertikale Hochskalieren** bietet dank der geringeren Serveranzahl eine größere Einfachheit, erhöht jedoch auch die Gefahr einer schwerwiegenderen Störung, wenn ein Server ausfällt.
- Das **horizontale Hochskalieren** erfordert eine größere Anzahl Server, teilt jedoch die Risiken auf so viele Server aus, dass im Falle eines Serverausfalls weniger Benutzer betroffen sind.

Aufgrund der größeren Stabilität wird das horizontale Hochskalieren empfohlen, d. h. das Erhöhen der Kapazität durch Hinzufügen zusätzlicher Server oder Knoten.

3.4.3 Hochverfügbarkeit

Hochverfügbarkeit bezeichnet die Fähigkeit eines Systems, selbst im Falle eines Fehlers im System weiterhin Services bereitzustellen. Hochverfügbarkeit wird erreicht, indem Schlüsselkomponenten des Systems redundant bereitgestellt werden.

> **Hinweis**
>
> Dieses Handbuch beschreibt das Bereitstellen der Hochverfügbarkeit der Kernservices von Host Access for the Cloud. Echte Hochverfügbarkeit beruht jedoch auf der Redundanz vieler verschiedener Ebenen in allen Systembereichen, was den Rahmen dieses Dokuments überschreitet.

Hochverfügbarkeit wird in Host Access for the Cloud auf folgende Weise erreicht:

- Bereitstellen einer ausreichenden Anzahl an Sitzungsservern und MSS-Servern, um die erforderliche Kapazität abzudecken und einen Toleranzbereich (Freiraum) für Ausfälle zu bieten
- Bereitstellen eines ausreichend großen Toleranzbereichs, um sicherzustellen, dass die verbleibenden Server im Falle eines Serverausfalls die zusätzliche Last bewältigen können
- Verwenden eines Lastverteilers, der die Last verteilt und die Benutzer im Falle eines Ausfalls zu anderen Servern leitet
- Replizieren von Daten zwischen MSS-Servern mittels MSS-Clustering

Der Abschnitt Beispielplan einer Hochverfügbarkeits-Bereitstellung stellt dar, wie diese Anforderungen erfüllt werden können.

3.4.4 Bestimmung der Anzahl der Sitzungsserver

Die Anzahl der erforderlichen Sitzungsserver hängt von der Anzahl der gleichzeitig ausgeführten Hostsitzungen ab. Hostsitzungen erzeugen eine größere Last auf dem Sitzungsserver als Benutzer.

Deshalb ist die Anzahl der erforderlichen Hostsitzungen von größerer Bedeutung als die Anzahl der Benutzer.

Anzahl der gleichzeitigen Hostsitzungen	Erforderliche Anzahl an Sitzungsservern
Bis 3000	2 Sitzungsserver
Mehr als 3000	(Anzahl der erforderlichen Hostsitzungen) / 2000 + 1 (mindestens drei)

- Ein einzelner Sitzungsserver unterstützt 2000 gleichzeitig verwendete Hostsitzungen.
- Ein Sitzungsserver bietet im Falle eines Failover-Szenarios einen Toleranzbereich für 1000 zusätzliche Hostsitzungen.
- Für Hochverfügbarkeitsbereitstellungen sind mindestens zwei Sitzungsserver erforderlich.

3.4.5 Bestimmung der Anzahl der MSS-Server

Anzahl gleichzeitiger Benutzer	Erforderliche Anzahl an MSS-Servern
Bis 30.000	3 MSS-Server
Mehr als 30.000	(Benötigte Benutzeranzahl) / 10.000 + 1 (muss eine ungerade Zahl sein)

- Ein einzelner MSS-Server unterstützt 10.000 gleichzeitige Benutzer.
- Ein MSS-Server bietet im Falle eines Failover-Szenarios einen Toleranzbereich für zusätzliche 5000 Benutzer.
- Für Hochverfügbarkeitsbereitstellungen sind mindestens 3 MSS-Server erforderlich
- Die Anzahl der MSS-Server in einer Hochverfügbarkeits-Bereitstellung muss ungerade sein, um die Anforderung eines Datenbankquorums zu erfüllen.

3.4.6 Verwendung von Lastverteilern

Sowohl für die Sitzungsserver als auch für MSS muss ein Lastverteiler bereitgestellt werden. Berücksichtigen Sie hierbei die folgenden allgemeinen Einstellungen:

- **Lastausgleichalgorithmus**: Der Algorithmus legt fest, zu welchem Server neuer Verkehr geleitet wird. Wir empfehlen eine Einstellung wie „Geringste Anzahl an Verbindungen“. Zur Gewährleistung der allgemeinen Systemstabilität sollte unbedingt überprüft werden, ob die Einstellung die Last ordnungsgemäß verteilt. Wenn der Lastverteiler nicht richtig konfiguriert ist oder nicht effizient ist, besteht die Gefahr der Überlastung einzelner Server.
- **Sitzungsbeständigkeit (Affinität/dauerhafte Sitzungen)**: Diese Einstellung beschreibt die Möglichkeit, einen bestimmten Benutzer über mehrere Anforderungen hinweg an den gleichen Server zu leiten. Sowohl der Sitzungsserver als auch MSS sind Stateful-Anwendungen (statusbehaftete Anwendungen) und erfordern die Aktivierung dauerhafter Sitzungen für die Lastverteiler.
- **Systemdiagnose-Endpunkt**: Dies bezeichnet die URL auf dem Zielservice, mit der ermittelt wird, ob die Instanz in gutem Zustand ist und weiterverwendet werden soll. Jeder Servertyp stellt eine eigene Systemdiagnose-URL bereit.

Der Abschnitt Beispielplan einer Hochverfügbarkeits-Bereitstellung enthält empfohlene Werte für jede dieser Einstellungen.

TLS-Optionen

Für die Handhabung von TLS in einem Lastverteiler gibt es drei übliche Optionen. Die Wahl der Option hängt von Ihren Anforderungen ab.

Für die ersten beiden Optionen muss das Zertifikat im Lastverteiler installiert sein. Bei der dritten Option, TLS-Passthrough, ist kein Zertifikat auf dem Lastverteiler erforderlich. Im Hochverfügbarkeits-Beispielplan wird TLS-Bridging verwendet, um durchgängiges TLS mit auf Cookies basierender Beständigkeit bereitzustellen. Folgende Optionen sind möglich:

- **TLS Termination/Offloading**: Bei dieser Option wird die HTTPS-Verbindung am Lastverteiler beendet und als HTTP-Verbindung zum Service fortgesetzt.
- **TLS-Bridging (Neuverschlüsselung)**: Bei dieser Option wird die HTTPS-Verbindung am Lastverteiler beendet und eine neue HTTPS-Verbindung zwischen Lastverteiler und Service wird hergestellt. Auf diese Weise wird durchgängiges TLS gewährleistet und der Lastverteiler kann dennoch einen Cookie für die Sitzungsbeständigkeit einfügen.
- **TLS-Passthrough (erforderlich für X.509)**: Der Lastverteiler agiert als Vertretung für die TLS-Verbindung, ohne sie zu entschlüsseln. Der Nachteil dieser Option besteht darin, dass kein Cookie eingefügt werden kann. Die Beständigkeit muss deshalb auf der Ursprungs-IP oder einem ähnlichen Parameter basieren.

TLS mit X.509-Single Sign-on

Bei der X.509-Authentifizierung ist die Option des TLS-Passthrough auf dem Host Access for the Cloud- und MSS-Lastverteiler erforderlich, weil den Servern im Back-End die Clientzertifikate präsentiert werden müssen. Weil TLS-Passthrough erforderlich ist, benötigen Sie eine nicht auf Cookies beruhende Methode zum Gewährleisten der Sitzungsbeständigkeit, zum Beispiel die Verwendung der Ursprungs-IP, für den Sitzungsserver- und MSS-Lastverteiler. Dies ist erforderlich, weil der Lastverteiler mit TLS-Passthrough die Verbindung nicht entschlüsseln kann und auch keinen Cookie setzen oder anzeigen kann.

3.4.7 Terminal ID Manager

Terminal ID Manager unterstützt zurzeit keine Hochverfügbarkeitsbereitstellungen. Sie können einen passiven Server einrichten, aber der Zustand der IDs wird nicht vom aktiven Server repliziert. Wenn der aktive Server nicht verfügbar ist, können Sie weiterhin auf den passiven Server zugreifen, die IDs behalten jedoch nicht ihren aktuellen Zustand bei.

3.4.8 Bereitstellungsoptionen

Zum Bereitstellen der Sitzungsserver haben Sie die Wahl zwischen zwei verschiedenen Verfahren:

1. Herkömmliches Installieren jedes Sitzungsservers auf einem dedizierten Server
2. Verwenden von Docker und Ausführen jedes Sitzungsservers in einem Container. Docker bietet verschiedene Vorteile, zum Beispiel eine größere Flexibilität in Bezug auf die Anzahl der Sitzungsserver, die auf einem einzelnen Server ausgeführt werden können. Weitere Informationen hierzu finden Sie unter Verwenden von Docker.

3.4.9 Grundlegendes zu Dienstunterbrechungen

> **Hinweis**
>
> Beachten Sie beim Auswählen der Bereitstellungsoptionen, dass HACloud aus mehreren Diensten besteht: Sitzungsserver, MSS und zugehörige Add-Ons, Terminal ID Manager und Nutzungsüberwachung. Standardmäßig werden MSS, Terminal ID Manager und die Nutzungsüberwachung zusammen in einem einzigen Prozess ausgeführt, können jedoch so konfiguriert werden, dass sie in separaten Prozessen ausgeführt werden. Der HACloud-Sitzungsserver wird immer als eigener Prozess ausgeführt.
>
> Wenn der Sitzungsserver beendet wird, werden alle Hostsitzungen auf diesem Server geschlossen. Benutzer, die bei diesem Server angemeldet waren, müssen sich erneut authentifizieren, wenn der Server neu gestartet wird oder sie zu einem neuen Server umgeleitet werden.

In dieser Tabelle werden die Auswirkungen auf die Fähigkeiten des Endbenutzers beschrieben, wenn Dienste nicht verfügbar sind oder neu gestartet wurden.

Aktion	Server nicht verfügbar	Server neu gestartet
MSS		
Anmelden	Nein	Ja
Neue Hostsitzungen erstellen	Nein	Ja
Vorhandene Hostsitzungen verwenden	Ja	Ja
Vorhandene Hostsitzungen wieder verbinden	Ja (ausgenommen SSH-Sitzungen)	Ja
Sitzungen bearbeiten	Nein	Ja (erneute Anmeldung erforderlich)
Benutzermakros aufzeichnen/ bearbeiten	Nein	Ja
Terminal ID Manager		
Hostsitzung verbinden, für die eine ID erforderlich ist	Nein	Ja
Hostsitzung verbinden, für die keine ID erforderlich ist	Ja	Ja
Nutzungsüberwachungsserver		
Neue Hostsitzungen erstellen	Nein*	Ja
Vorhandene Hostsitzungen verwenden	Ja	Ja

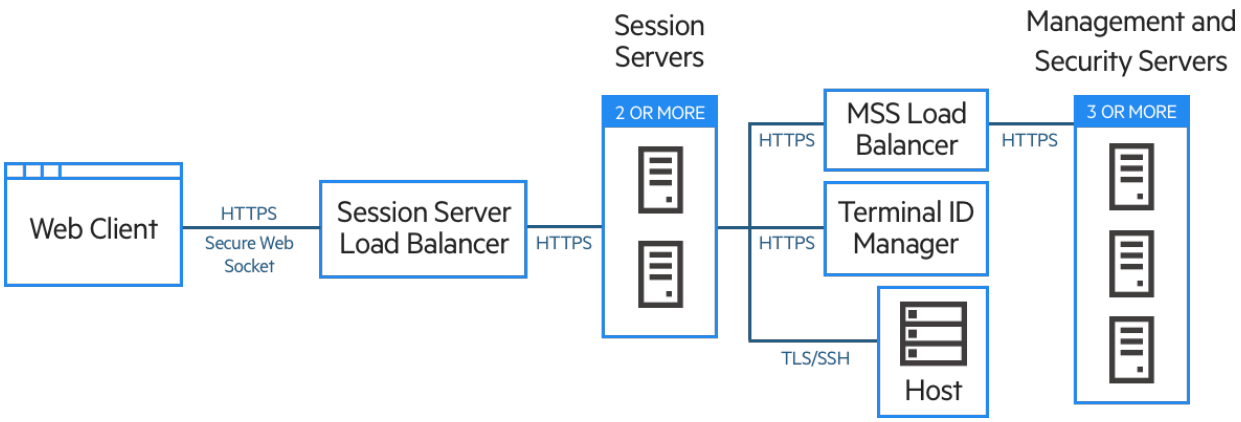
- Wenn die Eigenschaft `metering.host.required` auf „false“ festgelegt ist, können neue Sitzungen erstellt werden.

Wenn ein Sitzungsserver ausfällt, gehen alle Sitzungen für alle Benutzer verloren, die über den Lastverteiler mit diesem Sitzungsserver verbunden sind. Jeder Benutzer muss sich (über den Lastverteiler) bei einem anderen Sitzungsserver anmelden und neue Sitzungen starten.

3.5 Beispielplan einer Hochverfügbarkeits-Bereitstellung

Nachfolgend wird an einem Beispiel die skalierbare und auf sichere Weise ausgeführte Hochverfügbarkeits-Bereitstellung von Host Access for the Cloud beschrieben. Während die Details jeder Bereitstellung variieren (Sie können beispielsweise drei oder mehr Sitzungsserver bereitstellen), ist das Ziel hier, einen bekannt guten Ausgangspunkt zu beschreiben und allgemeine Fragen zur Bereitstellung zu beantworten.

3.5.1 Architektur



Die Bereitstellung besteht aus folgenden Komponenten:

- Sitzungsserver-Lastverteiler
- Zwei oder mehr Sitzungsserver
- MSS-Lastverteiler
- Drei oder mehr MSS-Server
- Terminal ID Manager
- LDAP- oder Identitätsmanagement-Server
- Host/Mainframe

3.5.2 Vorteile der Bereitstellung

An diesem Beispiel werden die folgenden Merkmale illustriert:

- Kapazität für bis zu dreitausend Hostsitzungen und Möglichkeit zur Skalierung nach Bedarf
- Hochverfügbarkeit der wesentlichen Services; Minimierung einzelner Ausfallpunkte und Verteilen der Last mittels Lastverteilern
- Fähigkeit zur Bewältigung des gleichzeitigen Ausfalls eines Sitzungsservers und eines MSS ohne wesentliche Minderung der Leistung am Webclient, dank integriertem Toleranzbereich
- Authentifizierungs- und Autorisierungsoptionen für MSS
- Sichere Kommunikation über HTTPS

3.5.3 Bereitstellungsschritte

MSS Für bestimmte Bereitstellungsschritte ist eine Konfiguration in der MSS-Verwaltungskonsole erforderlich.

Wir empfehlen, zum Bereitstellen die folgenden Schritte zu befolgen:

1. Grundlegendes Wissen zur Bereitstellung aneignen
2. Ressourcen basierend auf den Systemanforderungen und den Leitlinien zur Ermittlung der Systemgröße bereitstellen
3. MSS installieren und ein Cluster erstellen
4. MSS-Lastverteiler konfigurieren
5. Sitzungsserver installieren
6. Sitzungsserver-Lastverteiler konfigurieren
7. Authentifizierung und Autorisierung konfigurieren
8. Bereitstellung überprüfen

Informationen zu den Grundlagen der Bereitstellung, zu den Systemanforderungen und zur Ermittlung der Systemgröße haben Sie bereits in den vorigen Abschnitten erhalten.

3.5.4 Installieren von MSS

MSS Ausführliche Anweisungen finden Sie im MSS Installation Guide (MSS-Installationshandbuch).

Installieren Sie drei MSS-Server und konfigurieren Sie jeden zum Clustering. Die Dokumentation führt Sie durch den Prozess:

1. Öffnen Sie die Ports in der Firewall. Die von MSS und Host Access for the Cloud verwendeten Ports sind hier aufgelistet..
2. Installieren Sie MSS und dann die Host Access for the Cloud-Komponenten für MSS, indem Sie das Host Access for the Cloud-Installationsprogramm auf jedem MSS-Server ausführen.
3. Fügen Sie jeden Server zu einem Cluster hinzu.
4. Konfigurieren Sie auf jedem MSS-Server die allgemeinen Einstellungen, die Sicherheitseinstellungen und je nach Bedarf andere Einstellungen.

Weitere Informationen

- Ports
- MSS Installation Guide (MSS-Installationshandbuch)
- MSS Clustering (MSS-Clustering)

3.5.5 Konfigurieren eines MSS-Lastverteilers

MSS Verwenden Sie diese Werte zum Konfigurieren des MSS-Lastverteilers:

- **Lastausgleichalgorithmus:** geringste Anzahl an Verbindungen (oder ähnliche Einstellung)
- **Sitzungsbeständigkeit:**

  Konfigurieren Sie den MSS-Lastverteiler so, dass vorhandene Cookies und URL-Parameter für die Sitzungsbeständigkeit in der unten angegebenen Reihenfolge berücksichtigt werden:

  - Cookie **SESSIONID**
  - URL-Parameter **sessid** (nur erforderlich, wenn Single Sign-On über IIS als Authentifizierungsmethode konfiguriert ist)
  - Cookie **JSESSIONID**
  - URL-Parameter **jsessionid**
- **Systemdiagnose-Endgerät:** `https://<MSS-Server>/mss/actuator/health`
- **TLS:** Konfigurieren Sie TLS und installieren Sie je nach Bedarf Zertifikate.

Weitere Informationen

- MSS Using a Load Balancer (MSS – Verwendung eines Lastverteilers)

3.5.6 Installieren der Sitzungsserver

Installieren Sie zwei oder mehr Sitzungsserver.

Führen Sie für jeden Sitzungsserver die folgenden Schritte aus:

1. Öffnen Sie die Ports in der Firewall. Die von MSS und Host Access for the Cloud verwendeten Ports sind hier aufgelistet.
2. Installieren Sie den Sitzungsserver. Wählen Sie während der Installation die Verwendung eines MSS-Remoteservers und geben Sie die Adresse und den Port des MSS-Lastverteilers ein.
3. Importieren Sie das Sitzungserverzertifikat in den Truststore jedes vertrauenswürdigen MSS-Teilsystems: `system-trustcerts.bcfks`. Auf dem MSS-Server, der während der Installation vom Lastverteiler gewählt wurde, erfolgt dies automatisch. Auf den anderen Servern muss dies jedoch manuell ausgeführt werden. Es empfiehlt sich, auf jedem MSS-Server das Zertifikat zu importieren oder das Vorhandensein des Zertifikats zu überprüfen.

Weitere Informationen

- Ports
- Installation und Aufrüstung
- Sichern der Verbindungen

3.5.7 Konfigurieren des Sitzungsserver-Lastverteilers

Verwenden Sie beim Konfigurieren des Lastverteilers die folgenden Einstellungen:

- **Lastausgleichalgorithmus:** geringste Anzahl an Verbindungen (oder ähnliche Einstellung)
- **Sitzungsbeständigkeit:** aktiviert, JSESSIONID oder einen neuen Cookie verwenden Im Gegensatz zum MSS-Lastverteiler ist es hier nicht erforderlich, den vorhandenen JSESSIONID-Cookie zu verwenden.
- **Systemdiagnose-Endgerät:** `https://<session-server:7443>/actuator/health` Gehen Sie insbesondere für den Sitzungsserver mit Bedacht vor, während Sie konfigurieren, wie ein Knotenausfall ermittelt wird und was bei einem Ausfall geschehen soll. Wenn noch Benutzer mit der Instanz verbunden sind, verlieren diese Benutzer unter Umständen ihre Hostverbindungen. Um zu verhindern, dass eine Instanz vorzeitig als ausgefallen betrachtet wird, erwägen Sie höhere Werte für Zeitüberschreitungen und Wiederholungen. Einige Lastverteiler bieten einen Ausgleichmodus („drain mode“), bei dem vorhandene Benutzer verbunden bleiben können, neue Benutzer hingegen an andere Instanzen geleitet werden.
- **TLS:** Konfigurieren Sie TLS und installieren Sie je nach Bedarf Zertifikate.

3.5.8 Konfigurieren der Authentifizierung und Autorisierung

Detaillierte Informationen zum Wählen und Konfigurieren der Authentifizierung und Autorisierung finden Sie in Authentifizierung und Autorisierung

3.5.9 Überprüfen der Installation

Führen Sie die folgenden Schritte aus, nachdem Sie alle Komponenten installiert und konfiguriert haben:

- Melden Sie sich (über den MSS-Lastverteiler) bei der MSS-Verwaltungskonsole an.
- Wechseln Sie zu „Manage Sessions > Add a New Session“ (Sitzungen verwalten > Neue Sitzung hinzufügen) und erstellen Sie eine Testsitzung.
- Weisen Sie die Testsitzung einem Benutzer zu.
- Melden Sie sich als Testbenutzer über den Sitzungsserver-Lastverteiler beim Sitzungsserver an.
- Überprüfen Sie, ob die zugewiesene Sitzung verfügbar ist, geöffnet werden kann und eine Verbindung herstellen kann.

3.5.10 Konfigurieren von Single Sign-on (optional)

Im Folgenden werden einige zusätzliche Überlegungen erläutert, die beim Konfigurieren von Single Sign-On für eine Hochverfügbarkeits-Bereitstellung von Bedeutung sind.

SAML (Security Assertion Markup Language)

MSS Anweisungen zur SAML-Authentifizierung finden Sie im MSS Administrator Guide (MSS-Administratorhandbuch).

1. Importieren Sie das MSS-Lastverteilerzertifikat als verbürgtes Zertifikat in jeden MSS-Keystore `servletcontainer.bcfks`.
2. Aktualisieren Sie `management.server.url` in jeder MSS-Datei `container.properties` auf die MSS-Lastverteileradresse.
3. Legen Sie die Eigenschaft `management.server.callback.address` in jeder MSS-Datei `container.properties` auf eine Adresse fest, die der Sitzungsserver für eine bestimmte MSS-Instanz erreichen kann.
4. Starten Sie die MSS-Server neu.
5. Melden Sie sich bei der Verwaltungskonsole des aktiven MSS-Servers an, um die SAML-Authentifizierung zu konfigurieren. Überprüfen Sie, ob das MSS-Lastverteiler-DNS im Feld „Assertion consumer service prefix URL“ (Assertionsverbraucherdienst-Präfix-URL) verwendet wird, und fügen Sie den MSS- und Host Access for the Cloud-Lastverteiler-DNS zur SAML-Positivliste hinzu
6. Laden Sie die Metadaten des Dienstanbieters herunter und bearbeiten Sie sie, um jede MSS-Serveradresse als AssertionConsumerService einzufügen. Importieren Sie die aktualisierten Metadaten in den SAML-Identitätsanbieter. Beispiel:

```
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-loadbalancer:8443/mss/callback/SAML2Client" index="0"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-server-1:8443/mss/callback/SAML2Client" index="1"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-server-2:8443/mss/callback/SAML2Client" index="2"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-server-3:8443/mss/callback/SAML2Client" index="3"/`
```

7. Legen Sie das SameSite-Cookie-Flag auf „None“ (Keine) fest. Siehe Festlegen des SameSite-Attributs.

X.509

MSS Das MSS Administrator Guide (MSS-Administratorhandbuch) enthält X.509-Konfigurationsanweisungen.

In jedem Fall muss das verwendete Zertifikat über einen alternativen Antragstellernamen (SAN, Subject Alternative Name) verfügen, der alle DNS-Namen der MSS-Server und den DNS-Namen des Lastverteilers enthält.

1. Überprüfen Sie, ob die Firewall auf dem MSS-Server HTTP-Verkehr über den Port für beiderseitige Authentifizierung zulässt. Standardmäßig ist dies Port 8003.
2. Führen Sie auf jedem MSS die folgenden Schritte aus:
   - Ersetzen Sie das Zertifikat des Servlet-Engine-Eintrags in den `servletcontainer.bcfks`-Dateien.
   - Ersetzen Sie das Zertifikat des Systemeintrags in den `system-keystore.bcfks`-Dateien.
3. Importieren Sie das Zertifikat als vertrauenswürdiges Zertifikat in die Datei `trustcerts.bcfks` jedes Sitzungsservers.
4. Starten Sie MSS und die Sitzungsserver neu.
5. Konfigurieren Sie den MSS- und den HACloud-Lastverteiler zur Verwendung von TLS-Passthrough.
6. Konfigurieren Sie die X.509-Authentifizierung wie hier dokumentiert: „How to Configure X.509 Authentication“ (Konfigurieren der X.509-Authentifizierung).

3.5.11 Konfigurieren der Liste „Assigned Sessions“ (Zugewiesene Sitzungen)

Sie haben die Möglichkeit, die Liste „Assigned Sessions“ (Zugewiesene Sitzungen) zu verwenden, um neue Sitzungen zu starten. Dazu ist eine zusätzliche Konfiguration erforderlich:

- Konfigurieren Sie den MSS-Lastverteiler so, dass zuerst SESSIONID und dann die JSESSIONID-Cookies angehängt werden. Die Stickiness muss in dieser spezifischen Reihenfolge konfiguriert werden.
- Der Zugriff auf die Liste „Assigned Sessions“ (Zugewiesene Sitzungen) muss über den gleichen MSS-Lastverteiler erfolgen, über den auch der HACloud-Sitzungsserver eine Verbindung zu MSS herstellt.

Weitere Informationen:

- Bereitstellen von Zugriff auf Hostsitzungen
- Verwenden eines Lastverteilers

3.6 Installation und Aufrüstung

MSS Die MSS-Verwaltungskonsolenhilfe enthält im Abschnitt Product Activation (Produktaktivierung) Informationen zur Produktaktivierung.

Berücksichtigen Sie bei der Installation die unten aufgeführten Punkte.

- **Aktivierungsdateien**

  Aktivierungsdateien (activation.jaw) werden zum Aktivieren der Produktfunktionen verwendet. Das Installationspaket enthält zum Beispiel die Aktivierungsdatei, die zum Aktivieren der Kommunikation zwischen Host Access for the Cloud und MSS erforderlich ist. Die Aktivierung erfolgt üblicherweise im Rahmen des Installationsvorgangs. Aktivierungsdateien werden von der Micro Focus-Website für Downloads heruntergeladen und sind jeweils für die verschiedenen von Host Access for the Cloud unterstützten Editionen und Plattformen spezifisch. Zur Verwendung des Produkts in einer Produktionsumgebung muss es aktiviert werden.

  Falls die Aktivierung nicht Bestandteil der Installation war, müssen Sie die Verwaltungskonsole öffnen und den Aktivierungsvorgang abschließen („Configure Settings > Product Activation“ (Einstellungen konfigurieren > Produktaktivierung)). Informationen über das Handhaben von Aktivierungsdateien beim Aufrüsten finden Sie im Abschnitt zur Aufrüstung von früheren Versionen.

- **IIS-Reverseproxy mit Host Access for the Cloud**

  Wenn Sie den IIS-Reverseproxy verwenden möchten, lesen Sie die Informationen zu Voraussetzungen und Konfigurationsanweisungen in Zugriff auf Host Access for the Cloud mit IIS-Reverseproxy.

- **Sicherheit**

  Host Access for the Cloud unterstützt die TLS- und SSH-Protokolle zum Schutz sensibler Daten. Zum Sichern Ihrer Passwörter und von anderen vertraulichen Daten sollte in Browsern das HTTPS-Protokoll verwendet werden.

  Aus Sicherheitsgründen ist es vorteilhaft, Dienste als dedizierter Benutzer mit einem minimalen Satz von Berechtigungen auszuführen. Dies wird als Prinzip der geringsten Rechte bezeichnet.

  - Unter Linux sollten Sie HACloud und MSS als dedizierten Benutzer (Nicht-Root-Benutzer) mit eingeschränkten Rechten installieren.
  - Unter Windows müssen Sie zuerst das Produkt installieren und dann das System so anpassen, dass der Sitzungsserverdienst als dedizierter Benutzer mit eingeschränkten Rechten ausgeführt wird. Anweisungen hierzu finden Sie unter Ausführen des Sitzungsserverdiensts als dedizierter Benutzer mit eingeschränkten Berechtigungen.
  - Anweisungen zum Ausführen dieser Vorgehensweise in MSS.

3.6.1 Installation auf verschiedenen Plattformen

Host Access for the Cloud und Java

Sowohl der Sitzungsserver als auch MSS erfordern Java Version 11. Diese Java-Anforderung wird während der Installation erfüllt, außer für Systeme, die ein IBM-JDK erfordern (z. B. Linux auf System Z). Informationen zur Verwendung der nojdk-Option finden Sie unter „Installing on z/Linux“ (Installation unter z/Linux).

Host Access for the Cloud und MSS erfordern, dass die Java-Installation eine Verschlüsselung mit unbegrenzter Stärke unterstützt. Weitere Informationen finden Sie auf der Java-Website.

Gegebenenfalls können Sie mit den in der nojdk-Option angegebenen Umgebungsvariablen und INSTALL4J_JAVA_HOME_OVERRIDE eine bestimmte Java-Installation angeben.

Windows

Bei der Installation von Servern auf einer Windows-Plattform muss das Installationsprogramm von einem Administratorbenutzer mit Administratorberechtigungen ausgeführt werden. Eine einfache Windows-Installation wird unter Herunterladen und Installieren von Host Access for the Cloud beschrieben.

UNIX

- Sie müssen die Installation entweder als „Root“-Benutzer durchführen oder ein Benutzerkonto mit Root-Rechten verwenden. Nachdem die Installation erfolgreich durchgeführt wurde, kann die installierte Anwendung vom „Root“-Benutzer oder einem Benutzer, der als „Root“ ausgeführt wird, gestartet und verwaltet werden.
- Wenn Sie auf Linux-Plattformen arbeiten, führen Sie die nachstehenden Schritte aus, um den Sitzungsserver so einzurichten, dass er beim Systemstart automatisch gestartet wird.
- Zum Öffnen von Anwendungsports unter 1024 sind erweiterte Zugriffsrechte erforderlich. Host Access for the Cloud wird mit Verwendung einer niedrigeren Portnummer nur gestartet, wenn Sie über Systemrechte zum Öffnen von Ports mit niedrigeren Nummern verfügen.
- Mit dem chmod-Befehl können Sie anderen Benutzern als dem root-Benutzer Anwendungsrechte zuweisen.
- Wenn Sie die Installation unter einem Linux-System ohne Monitor durchführen und im System keine Schriftarten installiert sind, wird möglicherweise der folgende schriftartbezogene Fehler angezeigt: `java.lang.Error: Probable fatal error: No fonts found` (java.lang.Error: Wahrscheinlicher schwerwiegender Fehler: Keine Schriftarten gefunden). Stellen Sie sicher, dass fontconfig oder mindestens eine Schriftart auf dem System installiert ist, um mit der Installation fortfahren zu können.

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

Für Systeme, z. B. Linux on z Systems, die ein IBM-JDK erfordern, können Sie das nojdk-Installationsmedium verwenden, das kein gebündeltes JDK umfasst.

- Die Installation muss eine ausführbare Java-Datei zum Starten finden können. Wenn vom Installationsprogramm keine ausführbare Java-Datei gefunden wird, können Sie die Umgebungsvariable INSTALL4J_JAVA_HOME so festlegen, dass sie auf das bin-Verzeichnis einer Java-Installation verweist.
- Beim Start sucht das Installationsprogramm automatisch nach mit der Version kompatiblen JDKs im System. Wenn mehrere JDKs gefunden werden, wird eine Liste angezeigt, in der Sie ein JDK auswählen können. Wenn nur eine JRE im System gefunden wird, können Sie die Installation fortsetzen. Der Host Access for the Cloud-Server wird jedoch nur korrekt ausgeführt, nachdem Sie die Eigenschaft `wrapper.java.command` in `sessionserver/conf/container.conf` so aktualisiert haben, dass sie auf eine JDK-Installation verweist.

Gegebenenfalls können Sie mit den oben benannten Umgebungsvariablen und INSTALL4J_JAVA_HOME_OVERRIDE eine bestimmte Java-Installation angeben.

Unbeaufsichtigte Installation

Die Host Access for the Cloud-Installation basiert auf der install4j-Technologie, die unbeaufsichtigte Installationen unterstützt. Bei einer unbeaufsichtigten Installation können Sie das Produkt auf gleiche Weise auf mehreren Computern installieren.

So nutzen Sie die unbeaufsichtigte Installation:

1. Installieren Sie den Sitzungsserver mit dem automatischen Installationsprogramm auf einem Computer. Die Installation können Sie über die grafische Benutzeroberfläche oder im Konsolenmodus (-c) durchführen.

   Bei der Installation wird eine Textdatei mit dem Namen `response.varfile` erstellt, die die ausgewählten Installationsoptionen enthält. Die Datei befindet sich im Verzeichnis `[Sitzungsserver-Installationsverzeichnis]\.install4j\response.varfile`.

2. Kopieren Sie die Datei `response.varfile` auf einen anderen Computer, auf dem Sie den Sitzungsserver installieren möchten.

3. Suchen Sie die entsprechende ausführbare Datei zum Installieren des Produkts. Starten Sie das Installationsprogramm mit dem Argument `-q` und einem `-varfile`-Argument, das den Speicherort der Datei `response.varfile` angibt.

   Verwenden Sie beispielsweise zum Installieren des Sitzungsservers auf einer 64-Bit-Linux-Plattform mit der im gleichen Verzeichnis gespeicherten Datei „response.varfile“ den folgenden Befehl, wobei `<2.4.x.nnnn>` für die Produktversion und Buildnummer steht:

   ```
   hacloud-<2.4.x.nnnnn>-linuxx64.sh -q -varfile response.varfile
   ```

   Sie können auch die Option `-c` hinzufügen, um die Installation im Konsolenmodus durchzuführen, sodass Rückmeldungen wie „Dateien werden extrahiert“ und „Fertigstellen der Installation“ angezeigt werden.

3.6.2 Konfigurieren einer unvollständigen Installation

Wenn der Sitzungsserver entweder kein Zertifikat von MSS abrufen kann oder den Registrierungsprozess nicht abschließen kann, kann es zu einer unvollständigen Installation kommen. Befolgen Sie die Schritte zum Hinzufügen weiterer Sitzungsserver, um die Installation abzuschließen.

3.6.3 Aufrüsten von früheren Versionen

> **Vorsicht**
>
> Bei einer Aufrüstung ist es wichtig, dass Sie alle Aktivierungsdateien aus MSS entfernen, die früheren Versionen von Host Access for the Cloud zugeordnet sind. Wenn veraltete Aktivierungsdateien beibehalten werden, kann dies zu einem beschränkten Zugriff auf Sitzungen führen.

1. Sichern Sie vor dem Fortfahren alle Änderungen, die Sie an `hacloud\sessionserver\conf\container.properties` oder `hacloud\sessionserver\conf\container.conf` vorgenommen haben..
2. Installieren Sie Host Access for the Cloud.
3. Stellen Sie die in Schritt 1 gesicherten Dateien wieder her und starten Sie den Sitzungsserver neu.
4. Wenn dies nicht während des Installationsvorgangs erfolgt ist, installieren Sie die neuen Aktivierungsdateien über die Verwaltungskonsole unter „Configure Settings“ (Einstellungen konfigurieren) > „Product Activation“ (Produktaktivierung) in MSS.

Zusätzliche Konfiguration

Um serverseitige Ereignisse weiterzuverwenden, die in Reflection ZFE Version 2.3.2 oder früher erstellt wurden, kopieren Sie die serverseitigen JAR-Ereignisdateien aus `/webapps/zfe/WEB-INF/lib` zu `/microservices/sessionserver/extensions/server` und aktivieren Sie dann erneut die Erweiterungen.

3.6.4 Fehlerbehebung bei der Installation

Stellen Sie zum erfolgreichen Abschließen einer Installation sicher, dass Sie folgende häufige Probleme berücksichtigt haben:

✓ Sind die Aktivierungsdateien installiert und in der Verwaltungskonsole aktiviert?

In MSS werden Aktivierungsdateien zum Aktivieren der Produktfunktionen verwendet. Mit der Installation haben Sie eine Aktivierungsdatei erhalten, die dem Hosttyp für Ihre Verbindung zugeordnet ist. Wenn Sie beispielsweise über eine Lizenz für die Unisys Edition verfügen und dies nicht beim Installationsvorgang erfolgt ist, öffnen Sie die Verwaltungskonsole, navigieren Sie zu „Configure Settings“ (Einstellungen konfigurieren) > „Product Activation“ (Produktaktivierung) und überprüfen Sie, ob die Unisys-Aktivierungsdatei für Host Access for the Cloud vorhanden ist.

✓ Ist MSS für HTTPS konfiguriert?

Stellen Sie eine Verbindung mit dem System her, auf dem der Verwaltungsserver installiert ist, und melden Sie sich am Verwaltungsserver an. Öffnen Sie in der Verwaltungskonsole den Bereich „Einrichtung für Sicherheit“, und prüfen Sie die Protokollauswahl.

✓ Überprüfen Sie, ob MSS und Host Access for the Cloud verbürgte Zertifikate verwenden

MSS importiert Zertifikate und private Schlüssel in `C:\ProgramData\Micro Focus\MSS\MSSData\certificates`. Weitere Informationen finden Sie unter „Sichern der Verbindungen“. Wenn Sie keine verbürgten Zertifikate verwenden: Haben Sie Host Access for the Cloud zur Ausführung mit HTTP konfiguriert?

✓ Sind die Verbindungseigenschaften richtig konfiguriert?

Falls Sie die Verbindungsinformationen überprüfen müssen, können Sie die Datei `container.properties` der Verwaltungskomponente und des Sitzungsservers nutzen. Sie enthält die Verbindungseigenschaften, die für die Verbindung zwischen Sitzungsserver und MSS sowie zwischen Browser und Sitzungsserver erforderlich sind. Die Datei befindet sich in der Host Access for the Cloud-Installation unter `<Installationsverzeichnis>/sessionserver/conf/container.properties`.

✓ Installation wird unter UNIX- oder Linux-Plattformen nicht abgeschlossen

Aufgrund aktualisierter Verschlüsselungsbibliotheken kann es bei Installationen, die auf Servern ohne Monitor basieren, zu Systemverzögerungen kommen, wenn die Systementropie zu niedrig ist. Entropie bezeichnet die Menge an Zufallsdaten, die in einem Betriebssystem zur Verwendung bei der Verschlüsselung gesammelt wird. Diese Zufallsdaten werden oft aus Hardwarequellen gesammelt, zum Beispiel Mausbewegungen. Unzureichende Entropie kann dazu führen, dass der Installationsprozess hängt oder die Serverleistung beeinträchtigt ist. Bestimmte Plattformen installieren und aktivieren standardmäßig einen Entropiedienst und das Problem wird nicht bemerkt. Bei Bedarf kann eine Hardware- oder Softwarelösung das Problem beheben.

> **Tipp**
>
> Sie können die Entropiegenerierung mit dem Haveged-Werkzeug verbessern. Dieses Werkzeug unterstützt beim Bewältigen von Problemen mit geringer Entropie im Linux-Zufallszahlengenerator, die bei bestimmten Arbeitslasten und insbesondere auf monitorlosen Servern auftreten können. Weitere Informationen zu diesem Werkzeug finden Sie auf https://wiki.archlinux.org/index.php/Haveged.

Weitere Informationen finden Sie im Knowledgebase-Artikel Ensuring Sufficient Entropy to Avoid System Delays (Gewährleisten einer ausreichenden Entropie, um Systemverzögerungen zu vermeiden).

✓ Wird auf dem Server, auf dem Sie die Installation ausführen, aus Sicherheitsgründen der Zugriff auf das temporäre Verzeichnis verhindert?

Weitere Informationen zu diesem Problem finden Sie im Abschnitt zu Installationsproblemen, die bei verhindertem Zugriff auf das TEMP-Verzeichnis entstehen können, in Bekannte Probleme.

Tipp

Informationen zu weiteren bekannten Probleme und zur Fehlerbehebung finden Sie unter Technische Referenzen.

3.7 Ports

Die folgenden Ports werden in Host Access for the Cloud und MSS verwendet.

3.7.1 Host Access for the Cloud-Sitzungsserver

Port	Komponente	Fernzugriff erforderlich
7443	HTTPS – Web Client und zugehörige Connectors	Ja
32000-32001	Service Wrapper	Nein

3.7.2 Management and Security Server

Port	Komponente	Fernzugriff erforderlich
443	HTTPS – Verwaltungskonsole, Terminal ID Manager, Nutzungsüberwachung, Verwaltung der Nutzungsüberwachung	Ja
7001	Knotenübergreifende Kommunikation Cassandra TLS	Ja [1]
7199	Cassandra-JMX-Überwachung	Ja [1]
8000	X.509-Authentifizierung bei MSS über zentralisierte Verwaltung	[4]
8001, 8002	Tomcat AJP für die IIS-Integration	Ja [3]
8003	Vertrauenswürdiges X.509-Teilsystem	Ja [1]
8089	Nutzungsüberwachungsserver	Nein [2]
8761	Serviceregistrierung	Ja [1]
9042	Cassandra-Client- Port	Nein
9043	Cassandra Sidecar	Nein
32000-32001	Service Wrapper- Überwachung	Nein
44000	MSS-JMX-Überwachung	Nein
Zufällig	Zufälliger Port, der für MSS JMX RMI erforderlich ist	Nein
Zufällig	Zufälliger Port, der für Cassandra JMX RMI erforderlich ist	Nein

[1] Wird ausschließlich für die Backend-Kommunikation zwischen MSS und HACloud-Sitzungsservern verwendet

[2] Der Zugriff auf den Nutzungsüberwachungsdienst erfolgt in der Regel über Port 443

[3] Wird nur mit IIS-Integration verwendet

[4] Wird nicht von HACloud-Sitzungsservern verwendet

Die Ports für Host Access for the Cloud und für den MSS-Verwaltungsserver können entsprechend Ihren Netzwerkanforderungen geändert werden. Informationen zum Ändern der Ports des Sitzungsservers finden Sie unter Ändern der Ports.

3.8 Konfigurieren der Bereitstellung

3.8.1 Konfigurieren der Bereitstellung

Bei der Konfiguration der Bereitstellung von Host Access for the Cloud sind einige nach der Installation festzulegende Optionen und Sicherheitsüberlegungen zu berücksichtigen.

3.8.2 Authentifizierung und Autorisierung

Authentifizierung und Autorisierung

Authentifizierung und Autorisierung werden in HACloud über Host Access Management and Security Server (MSS) bereitgestellt und in der Verwaltungskonsole konfiguriert.

Bei der Authentifizierung wird die Identität des Benutzers basierend auf einem Berechtigungsnachweis überprüft, beispielsweise anhand einer Kombination aus Benutzername und Passwort oder anhand eines Clientzertifikats. Anschließend wird anhand der Autorisierung bestimmt, auf welche Sitzungen der Benutzer zugreifen kann.

HACloud unterstützt die folgenden Authentifizierungsmethoden: Keine, LDAP, Single Sign-on über IIS, Windows-Authentifizierung über Kerberos, Windows-Authentifizierung über NTLMv2 (veraltet), X.509-Clientzertifikate, SiteMinder und SAML.

Allgemeine Informationen zur Auswahl und zur Konfiguration der Authentifizierungs- und Autorisierungsmethoden finden Sie unter Authentication and Authorization (Authentifizierung und Autorisierung) in der MSS-Dokumentation.

Der Abschnitt Beispielplan einer Hochverfügbarkeits-Bereitstellung enthält zusätzliche wichtige Details zu bestimmten Authentifizierungsmethoden bei einer Bereitstellung in einer Hochverfügbarkeitsumgebung.

> **Hinweis**
>
> Bestimmte Authentifizierungsmethoden erfordern eine HACloud-spezifische Konfiguration. Weitere Informationen finden Sie in den Themen unter dieser Überschrift im Inhaltsverzeichnis.

Single Sign-on über IIS

MSS Weitere Informationen finden Sie bei Bedarf in Single Sign-on through IIS (Single Sign-on über IIS) in der Dokumentation der MSS-Verwaltungskonsole.

Diese Option verwendet den Microsoft IIS-Webserver.

Um Host Access for the Cloud für die Verwendung dieser Authentifizierungsmethode zu aktivieren, fügen Sie die folgende Eigenschaft in die Datei `<Installationsverzeichnis>/sessionserver/conf/container.properties ein` :

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

Der Wert dieser Eigenschaft besteht aus der Adresse und dem Port des IIS-Webservers sowie dem MSS-Pfad. Beispiel: `http://server/mss`. Wenn bei der Authentifizierung Fehler auftreten, müssen Sie möglicherweise den Domänennamen entfernen, damit die Domänenanmeldeinformationen an `IIS: http://server/mss` übergeben werden.

Windows-Authentifizierung – Kerberos

Kerberos ist ein Authentifizierungsprotokoll, das Verschlüsselungstickets verwendet, um das Übertragen von Klartextpasswörtern zu vermeiden. Clients erhalten Ticket-Granting-Tickets von Kerberos Key Distribution Center (KDC) und legen diese Tickets als Netzwerkberechtigung vor, um Zugriff auf Dienste zu erhalten.

In Host Access for the Cloud ermöglicht Kerberos Endbenutzern den Zugriff auf ihre Hostsitzungen auf dem Sitzungsserver, ohne zur Eingabe des Berechtigungsnachweises aufgefordert zu werden.

> **Hinweis**
>
> Die Kerberos-Authentifizierung bei AS/400-Hosts wird ebenfalls unterstützt, diese Funktionalität ist jedoch für die Authentifizierung von Endbenutzern für den Zugriff auf den Sitzungsserver noch nicht in Kerberos integriert.

Sie aktivieren und konfigurieren die Kerberos-Authentifizierung in MSS und aktivieren sie dann auf jedem Sitzungsserver in Ihrer Bereitstellung. Informationen zu den Anforderungen und weitere Informationen zum Konfigurieren und Verwenden von Kerberos finden Sie in der Kerberos-Dokumentation in MSS.

Im Folgenden sind die allgemeinen Schritte zur Verwendung der Kerberos-Authentifizierung in Host Access for the Cloud aufgeführt.

SCHRITTE ZUM AKTIVIEREN UND KONFIGURIEREN VON KERBEROS

1. Kerberos in MSS aktivieren und konfigurieren
2. Jeden HACloud-Sitzungsserver für Kerberos konfigurieren
3. Browser für Kerberos konfigurieren
4. Sitzungen starten

Kerberos auf dem Sitzungsserver konfigurieren

Um einen Sitzungsserver zur Ausführung von Kerberos zu konfigurieren, bearbeiten Sie die Datei „service.yml“ und fügen Sie das oauth-Profil hinzu:

1. Öffnen Sie die Datei `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/service.yml`.
2. Fügen Sie oauth zum Satz aktiver Profile hinzu:

```
- name: SPRING_PROFILES_ACTIVE
  value: tls, oauth
```

3. Starten Sie den Sitzungsserver neu.

Wenn Sie optional eine Hochverfügbarkeitsbereitstellung mit Lastverteilern konfigurieren, müssen Sie das oauth-Profil (vorheriger Schritt) und die folgenden Eigenschaften in der Datei „service.yml“ auf jedem Sitzungsserver konfigurieren.

1. Konfigurieren Sie die URL des MSS-Lastverteilers. Der Sitzungsserver leitet Benutzer zur Authentifizierung an diese URL um.

```
- name: AUTHSVC_HOST
  value: {HTTPS-URL des MSS-Lastverteilers}
```

2. Konfigurieren Sie den Domänennamen des Sitzungsserver-Lastverteilers. MSS adressiert wieder an diesen Server um, nachdem ein Benutzer authentifiziert wurde.

```
- name: PROXY_DOMAIN
  value: {FQDN des Sitzungsserver-Lastverteilers}
```

3. Konfigurieren Sie den Port, der beim Zugriff auf den Sitzungsserver über den Lastverteiler des Sitzungsservers verwendet wird.

```
- name: PROXY_PORT
  value: {Portnummer auf dem Sitzungsserver-Lastverteiler}
```

4. Starten Sie den Sitzungsserver neu.

Beispiel

```
    - name: SPRING_PROFILES_ACTIVE
      value: tls, oauth
    (Bei Verwendung von Lastverteilern ...)
    - name: AUTHSVC_HOST value: https://mss-load-balancer.mydomain.com
    - name: PROXY_DOMAIN
      value: sessionserver-load-balancer.mydomain.com
    - name: PROXY_PORT
      value: 7443
```

Browser für Kerberos konfigurieren

Um sich mit Kerberos anzumelden, muss Ihr Browser ordnungsgemäß für die Windows-Authentifizierung über Kerberos konfiguriert sein und Ihr Computer muss Mitglied der richtigen Domäne (Kerberos-Bereich) sein. Anweisungen zum Aktivieren von Kerberos finden Sie in der Hilfe Ihres jeweiligen Browsers.

Sitzungen starten

> **Hinweis**
>
> Die Kerberos-Authentifizierung wird zurzeit von der Liste der zugewiesenen Sitzungen nicht unterstützt. Sie ist nur beim Zugriff über den Sitzungsserver verfügbar.

HACloud-Sitzungen benötigen keine zusätzliche Konfiguration zum Starten und Authentifizieren über Kerberos, sofern Ihr Browser korrekt für die Windows-Authentifizierung/Kerberos konfiguriert ist. Navigieren Sie einfach zu https://session-server-lb.mydomain.com:7443 und Sie werden automatisch beim HACloud-Sitzungsserver angemeldet.

SAML

SAML (Security Assertion Markup Language) ist ein XML-basiertes Format nach offenen Standards, das Authentifizierungs- und Autorisierungsdaten zwischen einem Identitätsanbieter (dem Server, der SAML-Assertionen ausgibt und die Authentifizierung durchführt) und einem Dienstanbieter (dem Webserver, von dem aus Sie auf Informationen oder Dienste zugreifen) austauscht. MSS fungiert als Dienstanbieter.

MSS Weitere Informationen finden Sie bei Bedarf unter SAML Configuration Steps (SAML-Konfigurationsschritte) in der Dokumentation der MSS-Verwaltungskonsole.

> **Hinweis**
>
> Das SameSite-Flag muss angepasst werden, wenn SAML hinter einem Lastverteiler verwendet wird. Siehe Festlegen des SameSite-Attributs.

BEHEBEN VON FEHLERN IN DER KONFIGURATION

Informationen zu Authentifizierungsproblemen und Sitzungstimeoutfehlern finden Sie unter Troubleshooting SAML Setup (Behebung von Fehlern der SAML-Einrichtung) im MSS Administrator Guide (MSS-Administratorhandbuch).

X.509-Authentifizierung

Mit der X.509-Clientauthentifizierung können sich Clients über Zertifikate anstatt mit einem Benutzernamen und Passwort bei Servern authentifizieren. Hierzu wird der Standard X.509 PKI (Public Key Infrastructure; Infrastruktur für öffentliche Schlüssel) verwendet.

MSS bietet zusätzliche Informationen zur X.509-Konfiguration.

X.509-CLIENTAUTHENTIFIZIERUNG AKTIVIEREN

- Wenn der Benutzer mit TLS auf den Webclient zugreift, sendet der Browser ein Zertifikat an den Sitzungsserver, das den Endbenutzer identifiziert und den TLS-Handshake abschließt.
- Der Sitzungsserver überprüft das Clientzertifikat und dessen Verbürgung über den Truststore.
- Nach Abschluss der TLS-Verhandlung (wenn der Sitzungsserver den Endbenutzer verbürgt hat) sendet der Sitzungsserver das öffentliche Zertifikat des Endbenutzers zur weiteren Überprüfung an MSS.
- MSS überprüft ebenfalls über den eigenen Truststore, ob das Zertifikat des Endbenutzers verbürgt werden kann.
- Nach Abschluss der Überprüfung durch MSS ist der Benutzer erfolgreich authentifiziert.

Die gesamte Zertifikatskette des Client muss im Sitzungsserver-Truststore und im MSS-Truststore vorhanden sein oder von einer Zertifizierungsstelle signiert sein, die in beiden Truststores enthalten ist.

Der Browser ermittelt das zu sendende Clientzertifikat gemäß der Browser- oder Smartcard-spezifischen Konfiguration.

Grundlegende Schritte

1. Verbürgen Sie die Zertifikate auf dem Sitzungsserver und in MSS, sofern sie noch nicht verbürgt sind.
2. Starten Sie die Server neu.
3. Konfigurieren Sie X.509 in der MSS-Verwaltungskonsole.

Zertifikat in MSS und auf dem Sitzungsserver verbürgen

- Zertifikat in MSS verbürgen

  Ihr Zertifikat der Zertifizierungsstelle kann bereits im vertrauenswürdigen Speicher von MSS enthalten sein. Dies kommt häufig bei bekannten Zertifizierungsstellen vor. In dem Fall können Sie diesen Schritt überspringen.

  Überprüfung:

- Öffnen Sie die Verwaltungskonsole, klicken Sie auf „Configure Settings“ (Einstellungen konfigurieren), und öffnen Sie die Registerkarte „Trusted Certificates“ (Verbürgte Zertifikate).

Öffnen Sie „Trusted Root Certificate Authorities“ (Verbürgte Stammzertifizierungsstellen), um eine Liste der verfügbaren Zertifikate anzuzeigen.

- Wenn Ihr Zertifikat nicht aufgelistet ist, müssen Sie entsprechend den Eingabeaufforderungen und der Dokumentation in der Verwaltungskonsole die signierende Stammzertifizierungsstelle in MSS installieren.
- Zertifikat auf dem Sitzungsserver verbürgen

  So installieren Sie das Zertifikat auf dem Sitzungsserver:

  Importieren Sie das Zertifikat in `<Installationsverzeichnis>\sessionserver\etc`:

```
keytool -importcert -file <cert-Datei> -alias <alias-unter-dem-Zertifikat-gespeichert-werden-soll>
-keystore trustcerts.bcfks -storetype bcfks -providername BCFIPS
-providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
-providerpath ../lib/bc-fips-*.jar
-storepass changeit
```

Alle Server neu starten

Die Konfiguration ist erst wirksam, nachdem Sie alle Server neu gestartet haben.

X.509 mit LDAP-Failover in der MSS-Verwaltungskonsole konfigurieren

Nachdem die Zertifikate eingerichtet sind, können Sie X.509 mit der Option zum Fallback auf die LDAP-Authentifizierung in Management and Security Server Administrative Console | Configure Settings | Authentication & Authorization (Management and Security Server-Verwaltungskonsole | Einstellungen konfigurieren | Authentifizierung und Autorisierung) konfigurieren. Beschreibungen der Konfigurationsoptionen finden Sie in der Onlinehilfe der Verwaltungskonsole.

AKTIVIEREN VON X.509 ÜBER EINEN LASTVERTEILER, DER ZUM BEENDEN DER TLS-VERBINDUNG KONFIGURIERT IST

In dieser Konfiguration authentifiziert der Lastverteiler die Endbenutzer durch Bestätigung des Clientzertifikats. Das Clientzertifikat muss jedoch weiterhin an alle anderen MSS-Systeme gesendet werden, um den eingehenden Benutzer zu identifizieren.

Wenn der Lastausgleicher zum Beenden der TLS-Verbindung konfiguriert ist, kann das Zertifikat des Benutzers zu einem HTTP-Header hinzugefügt, vom Sitzungsserver extrahiert und dann zur Autorisierung an MSS weitergeleitet werden. Um das Zertifikat in einen Header zu übertragen, legen Sie zuerst in der Datei `container.properties` des HACloud-Sitzungsservers den Headernamen fest:

So übertragen Sie das Zertifikat an einen Header:

1. Legen Sie den Headernamen in der Datei „container.properties“ des HACloud-Sitzungsservers fest:

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

2. Legen Sie den Headerwert auf das Benutzerzertifikat in der Lastausgleicherkonfiguration fest. Beispiel mit Verwendung einer BIG-IP-iRule:

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

Dies setzt voraus, dass `$client_cert` auf das Benutzerzertifikat im PEM-Format festgelegt wurde. Wenn das Benutzerzertifikat im DER-Format vorliegt, verwenden Sie die Base64-Kodierung:

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

Durch das Kodieren des Zertifikats wird gewährleistet, dass der Headerwert eine Zeile ASCII-Text darstellt. Dies ist erforderlich, damit der HACloud-Sitzungsserver den Wert lesen kann.

> **Hinweis**
>
> Die Authentifizierung mit dem Clientzertifikat muss weiterhin zwischen dem Lastverteiler und dem Sitzungsserver stattfinden. Der Lastverteiler muss so konfiguriert sein, dass er sein Zertifikat an den Sitzungsserver sendet, und die Zertifizierungsstelle des Lastverteilers muss im Truststore des Sitzungsservers vorhanden sein.

3. Nachdem Sie den Lastausgleicher zum Senden des Zertifikats an den HACloud-Sitzungsserver konfiguriert haben und das Hinzufügen des Benutzerzertifikats zum Header konfiguriert haben, starten Sie den Sitzungsserver neu.

Bei der Verbindung mit einem Zertifikat oder einer Smartcard über den Lastausgleicher wird der vom Zertifikat dargestellte Benutzer erfolgreich authentifiziert und autorisiert. Um den Vorgang zu überprüfen, legen Sie den Protokollierumfang des Sitzungsservers auf „DEBUG“ (Fehlersuche) fest und untersuchen Sie die Datei „sessionserver.log“ auf Einträge der folgenden Art:

```
Attempting to extract certificate from X-SSL-Client-Cert header. User <DN-Wert> has been preauthenticated from <IP-Adresse>
(Es wird versucht, das Zertifikat vom X-SSL-Client-Cert-Header abzurufen. Der Benutzer <DN-Wert> wurde von <IP-Adresse> vorauthentifiziert.)
```

Zusätzliche Konfiguration

Standardmäßig enthält der Truststore des HACloud-Sitzungsservers die Java-ZS-Zertifikate. Deshalb akzeptiert der HACloud-Sitzungsserver jedes Clientzertifikat, das von einer bekannten Zertifizierungsstelle signiert ist. Um sicherzustellen, dass nur die gewünschten Lastausgleicher eine Verbindung zum Sitzungsserver herstellen können, müssen Sie die Java-ZS-Zertifikate aus dem Truststore entfernen und sicherstellen, dass nur die erforderlichen Zertifikate im Truststore installiert sind.

Um die zulässigen Clientzertifikate nach Aussteller-DN zu filtern, legen Sie in der Datei `container.properties` des HACloud-Sitzungsservers die folgenden Eigenschaften fest:

```
X509.client.cert.issuer=<DN-Wert>
X509.client.cert.subject=<Subject-DN-Wert>
X509.client.cert.serial=<Seriennummer>
X509.client.cert.sha1=<SHA1-Fingerabdruck>
X509.client.cert.sha256=<SHA256-Fingerabdruck>
```

Die DN-Werte müssen genau mit dem Lastausgleich-Zertifikataussteller bzw. Subject-DN übereinstimmen. Die Seriennummer muss einen Dezimalwert (Zehnersystem) annehmen. Die Werte für den SHA1- und den SHA256-Fingerabdruck müssen im Hexadezimalformat eingegeben werden. Wenn beliebige dieser Attribute festgelegt sind, wird überprüft, ob die Attribute des

eingehenden Zertifikats mit den angegebenen Eigenschaftenwerten übereinstimmen. Wenn beliebige Werte nicht übereinstimmen, erfolgt keine Autorisierung.

3.8.3 Nutzungsüberwachung einrichten

MSS bietet Nutzungsüberwachungsfunktionen zum Überwachen von Hostsitzungen. Weitere Informationen finden Sie unter Metering (Nutzungsüberwachung).

Management and Security Server stellt Nutzungsüberwachungsfunktionen für Hostsitzungen bereit.

Überprüfen Sie vor der Konfiguration der Nutzungsüberwachung für Host Access for the Cloud, ob die Nutzungsüberwachungsfunktion für MSS aktiviert ist. Vollständige Anweisungen finden Sie im Installation Guide (Installationshandbuch/).

Die Nutzungsüberwachung ist in Host Access for the Cloud global für alle Emulationssitzungen festgelegt, die vom Sitzungsserver erstellt werden. Die Einstellungen werden in der Datei `sessionserver/conf/container.properties` konfiguriert.

Eigenschaft	Beschreibung
metering.enabled	Aktiviert bzw. deaktiviert die Nutzungsüberwachung mit den Werten „true“ und „false“. Wenn der Wert nicht auf „true“ gesetzt ist, wird die Nutzungsüberwachung deaktiviert.
metering.host.required	Gibt an, ob die Sitzung auch dann eine Verbindung zum Host herstellen kann, wenn der Nutzungsüberwachungsserver nicht erreichbar ist. „True“ bedeutet, dass keine Verbindungen zu Sitzungen hergestellt werden können, wenn der Nutzungsüberwachungsserver nicht erreichbar ist. „False“ bedeutet, dass auch bei nicht erreichbarem Nutzungsüberwachungsserver Verbindungen zu Sitzungen hergestellt werden können.
metering.server.url	Gibt den Namen bzw. die Adresse des Nutzungsüberwachungsservers, den Port, das Protokoll und den Webapp-Kontext an. Die Syntax lautet `host:port|protokoll|kontext"`. Sie entspricht der Syntax, die der MSS-Server in der Datei `MssData/serverconfig.props` für die Registrierung der Nutzungsüberwachungsserver verwendet hat. Dabei muss im Bereich „host:port“ der URL das Zeichen „:“ manuell geschützt werden. Beispiel: `10.10.11.55\:443`.

Beispielerweiterungen zu `sessionserver/conf/container.properties`

```
metering.enabled=true
metering.host.required=false
metering.server.url=10.10.11.55\:443|https|meter
```

Hinweis

Wenn Sie versuchen, eine Verbindung herzustellen, während alle Lizenzen in Verwendung sind, wird die Sitzung getrennt. Anhand der Informationen in der Datei `<Installationsverzeichnis>/sessionserver/logs/sessionserver.log` können Sie ermitteln, ob der Host die Verbindung getrennt hat oder ob der Nutzungsüberwachungsservice die Verbindung gestoppt hat.

3.8.4 Terminal ID Manager einrichten

MSS Zum Einrichten von Terminal ID Manager muss diese Funktion in MSS aktiviert sein (siehe Setting up the Terminal ID Manager (Einrichten von Terminal ID Manager)).

Management and Security Server stellt das Terminal ID Management-Add-On zum Zusammenfassen von Terminalkennungen in Pools, zum Verfolgen der Kennungsnutzung und zum Verwalten der Wartezeiten bei Inaktivität für bestimmte Benutzer bereit, wodurch die Terminalkennungsressourcen effizienter genutzt und die Betriebskosten erheblich gesenkt werden können.

Für das Terminal ID Management-Add-On ist eine separate Lizenz erforderlich.

Bevor Sie mit der Konfiguration von Terminal ID Manager für Host Access for the Cloud beginnen, überprüfen Sie, ob diese Option für MSS aktiviert ist. Ausführliche Anweisungen zu diesem Thema finden Sie im Installationshandbuch für MSS.

> **Tipp**
>
> Wenn MSS und Host Access for the Cloud auf demselben Computer installiert sind, ist keine weitere Konfiguration erforderlich.

Terminal ID Manager für Host Access for the Cloud konfigurieren

Stellen Sie die richtige Adresse für Terminal ID Manager bereit, um Terminal ID Manager für Host Access for the Cloud zu konfigurieren.

1. Öffnen Sie die Datei `sessionserver/conf/container.properties`.
2. Aktualisieren Sie `id.manager.server.url=http://localhost:443/tidm` gemäß der in Management and Security Server konfigurierten Adresse für Terminal ID Manager.
3. Starten Sie den Sitzungsserver neu.

3.8.5 Einrichten von Automated Sign-On for Mainframe

MSS Automated Sign-On for Mainframe – Administrator Guide (Automated Sign-On for Mainframe – Administratorhandbuch) enthält weitere Informationen zur Konfiguration dieser Option.

Automated Sign-On for Mainframe ist ein Add-On-Produkt für Management and Security Server, mit dem sich Endbenutzer bei einem Terminalemulationsclient authentifizieren können und automatisch bei einer Hostanwendung im z/OS-Mainframe angemeldet werden.

1. Installieren und konfigurieren Sie das Automated Sign-On for Mainframe-Add-on für Management and Security Server. Vollständige Anweisungen finden Sie im Automated Sign-On for Mainframe – Administrator Guide (Automated Sign-On for Mainframe – Administratorhandbuch).
2. Nachdem Sie Management and Security Server eingerichtet haben, öffnen Sie die Verwaltungskonsole, um Sitzungen hinzuzufügen und diesen Sitzungen Benutzer zuzuordnen. Während dieses Vorgangs können Sie die zusätzlichen Konfigurationsschritte abschließen, die für die Implementierung von Automated Sign-On erforderlich sind.
3. Ein Host Access for the Cloud-Makro sendet den Mainframe-Benutzernamen des Benutzers und das Weiterleitungsticket an die Hostanwendung. Der Benutzer wird dann automatisch angemeldet. Unterstützung bei der Erstellung des Makros:
   - Die Makro-API enthält das Objekt AutoSignon, das die Methoden bereitstellt, die für die Erstellung einer Host Access for the Cloud-Anmeldung zur Verwendung mit der Automated Sign-On for Mainframe-Funktion erforderlich sind.
   - Sie können auch das Automatic Sign-On Macro for Mainframes-Beispielmakro referenzieren. Dieses Makro verwendet das AutoSignon-Objekt zum Erstellen eines Makros, das mithilfe des Berechtigungsnachweises eines Benutzers ein Weiterleitungsticket von Digital Certificate Access Server (DCAS) abruft.

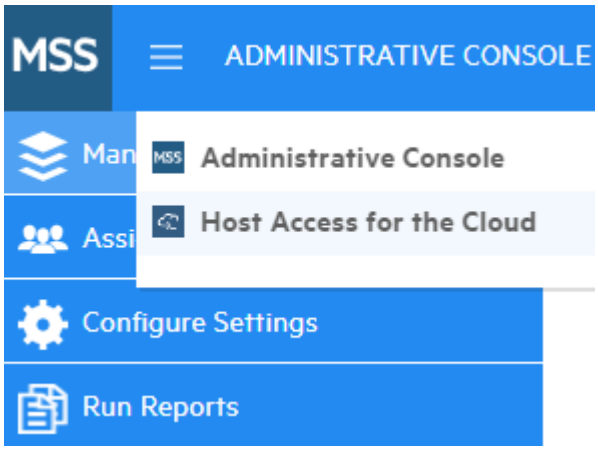
3.8.6 Einrichten von Kerberos für Single Sign-on mit AS/400

Kerberos ist ein Authentifizierungsprotokoll, das Verschlüsselungstickets verwendet, um das Übertragen von Klartextpasswörtern zu vermeiden. Clientservices erhalten Ticket-Granting-Tickets von Kerberos Key Distribution Center (KDC) und legen diese Tickets als Netzwerkberechtigung vor, um Zugriff auf Dienste zu erhalten.

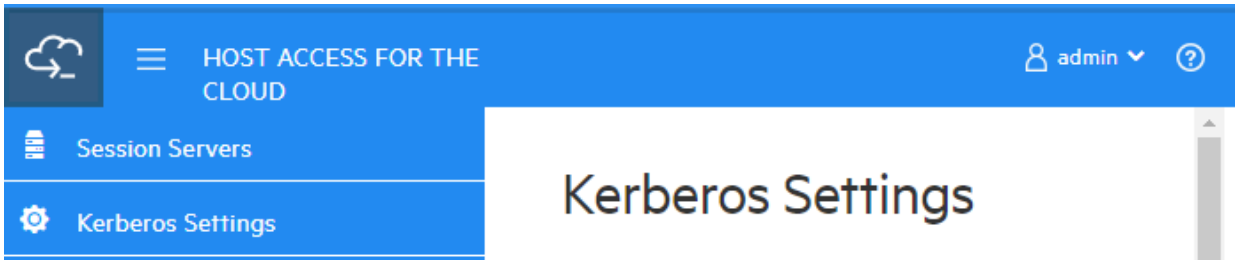
> **Hinweis**
>
> Die Kerberos-Authentifizierung wird für Endbenutzer, die auf den Sitzungsserver zugreifen, ebenfalls unterstützt, diese Funktionalität ist jedoch noch nicht in Kerberos für die AS/400-Authentifizierung integriert. Diese Funktion ermöglicht die automatische Anmeldung vom Sitzungsserver bei einem AS/400-Host. MSS muss mit einer Authentifizierungsmethode konfiguriert werden, die ein Benutzerprinzipal generiert, das in der Active Directory-Domäne von Kerberos aufgelöst werden kann, zum Beispiel LDAP, SAML oder SiteMinder. Ein Windows Active Directory-Server ist erforderlich.

Mit der Verwendung von Kerberos müssen die Benutzer nach einer anfänglichen Anmeldung bei der Domäne nicht erneut ihren Berechtigungsnachweis eingeben, um auf die AS/400-Sitzungen in Host Access for the Cloud zuzugreifen.

Einen Überblick über die Aktivierung und Verwendung dieser Funktion finden Sie in der Dokumentation im Bereich „MSS-Verwaltungskonsole > Host Access for the Cloud“.



Wählen Sie „Host Access for the Cloud“ in der Dropdown-Liste, wählen Sie dann „Kerberos Settings“ (Kerberos-Einstellungen) aus und klicken Sie auf die Hilfe-Schaltfläche:



3.9 Sichern der Verbindungen

3.9.1 Sichere Verbindungen

Host Access for the Cloud verwendet Transport Layer Security (TLS) für die verschlüsselte, sichere Kommunikation zwischen Client-Webbrowsern, Sitzungsservern, MSS und Back-End-Hosts.

Überblick

Public Key Infrastructure (PKI)

TLS verwendet PKI (Public Key Infrastructure; Infrastruktur für öffentliche Schlüssel) zur Implementierung der Sicherheit. PKI verwendet öffentliche und private Schlüssel, um die Client- und Serverkommunikation zu sichern. Öffentliche und private Schlüssel sind aus mathematischer Sicht ähnlich, weisen jedoch einige Unterschiede auf. Eine mit einem öffentlichen Schlüssel verschlüsselte Nachricht kann nur mit dem privaten Schlüssel entschlüsselt werden. Zusammen werden diese Schlüssel als Schlüsselpaar bezeichnet.

Zertifikate

Digitale Zertifikate sind Berechtigungsnachweise, die zur Überprüfung von Personen, Computern und Netzwerken verwendet werden. Sie stellen die Verknüpfung zwischen einem öffentlichen Schlüssel und einer Organisation dar, die von einem verbürgten Dritten, einer sogenannten Zertifizierungsstelle, überprüft (signiert) wurde. Mithilfe digitaler Zertifikate lassen sich öffentliche Verschlüsselungsschlüssel bequem verteilen.

Keystores

Zertifikate und private Schlüssel werden in Java-Keystores gespeichert. Keystore-Eintrage werden mit einer eindeutigen Kennung, dem sogenannten Alias, identifiziert. Oft werden private Schlüssel und Zertifikate mit ihrem entsprechenden öffentlichen Schlüssel separat von den Zertifikaten gespeichert, die von den zu Verbürgungszwecken eingesetzten Dritten empfangen werden. Dieser separate Keystore wird als Truststore bezeichnet. Ein Truststore enthält Zertifikate von möglichen Kommunikationspartnern oder von Zertifizierungsstellen, die zur Identifizierung von Dritten eingesetzt werden.

Standardmäßige sichere Installation

Während der Installation von Host Access for the Cloud und MSS werden eigensignierte Zertifikate generiert, ausgetauscht und dann zum Sichern der gesamten Kommunikation zwischen Sitzungsserver, Webbrowsern und MSS verwendet. Eigensignierte Zertifikate sind Identitätszertifikate, die von der Entität signiert sind, deren Identität sie zertifizieren.

Sowohl Sitzungsserver als auch MSS-Server verwenden ihre generierten eigensignierten Zertifikate, um sich bei Remoteclients wie Webbrowsern und anderen Sitzungsservern oder MSS-Servern zu

identifizieren. Diese eigensignierten Zertifikate und die zugehörigen privaten Schlüssel werden in den entsprechenden Keystores gespeichert.

Um die sichere Kommunikation zwischen den Clients (Webbrowser, Sitzungsserver und MSS-Server) abzuschließen, müssen die Clients das generierte eigensignierte Zertifikat verbürgen. Der Sitzungsserver verbürgt das MSS-Zertifikat während der Installation und speichert es im eigenen Truststore. Auf die gleiche Weise ruft MSS während der Installation das Zertifikat des Sitzungsservers ab und speichert es im eigenen Truststore.

Siehe Vom Sitzungsserver verwendete Stores

MSS Die MSS-Verwaltungskonsolenhilfe enthält im Abschnitt General Security and Certificates (Allgemeine Sicherheit und Zertifikate) detaillierte Informationen zur allgemeinen Sicherheit und zu Zertifikaten.

3.9.2 Vom Sitzungsserver verwendete Stores

Identitätszertifikate

Die Identitätszertifikate für jeden Servertyp sind an den folgenden Orten außerhalb der unten genannten Keystores verfügbar.

- HACloud-Sitzungsserverzertifikat: `HACloud/sessionserver/etc/<Computername>.cer`
- MSS-Zertifikat: `MSS/server/etc/<Computername>.cer`

Keystore und Truststore des Sitzungsservers

Die vom Sitzungsserver verwendeten Keystores und Truststores werden in der folgenden Tabelle beschrieben.

- Speicherort: `HACloud/sessionserver/etc/`
- Typ: `bcfks` (Bouncy Castle FIPS-Keystore)
- Standardmäßiges Passwort: `changeit`

Keystore	Funktion
keystore.bcfks	• Berechtigungsnachweisspeicher für eingehende TLS-Verbindungen • Enthält das vom Sitzungsserver bereitgestellte Zertifikat • Wird für eingebetteten Webserver verwendet (Jetty) • Wird beim Start erstellt
trustcerts.bcfks	• Truststore für ausgehende TLS-Verbindungen • Wird zum Überprüfen der Server verwendet, mit denen der Sitzungsserver eine Verbindung herstellt, z. B. MSS • Truststore zum Überprüfen eingehender Lastverteiler-Verbindungen bei Verwendung der X.509-Authentifizierung über einen Lastverteiler • Wird beim Start erstellt

> **Hinweis**
>
> Die Verbürgung für Hostemulationsverbindungen wird von MSS verwaltet. Weitere Informationen hierzu finden Sie in Sichere Emulationsverbindung zu einem verbürgten Host herstellen.

So ändern Sie ein Keystore- oder Truststore-Passwort

Aktualisieren Sie in `HACloud/sessionserver/conf/container.properties` die folgenden Einstellungen:

- `server.ssl.key-Store-Passwort`
- `server.ssl.trust-store-password`

Aus Sicherheitsgründen ist es am besten, ein verschleiertes Passwort zu verwenden. Um eines zu generieren, führen Sie den folgenden Befehl aus dem Verzeichnis HACloud/sessionserver aus:

```
../java/bin/java -cp ./lib/jetty-util-<Version>.jar
org.eclipse.jetty.util.security.Password zuVerschleierndesPasswort
```

3.9.3 Werkzeuge

- KeyStore Explorer – Mit dem KeyStore Explorer-Dienstprogramm können Sie eine einfache Benutzeroberfläche zum Erstellen von Zertifizierungsanträgen und Importieren von ZS-signierten Zertifikaten in Host Access for the Cloud bereitstellen.
- Um KeyStore Explorer unter Windows zu starten, führen Sie `\HACloud\utilities\keystore-explorer.bat` als Administrator oder mit Verwaltungsrechten aus.
- Um KeyStore Explorer unter UNIX zu starten, führen Sie `hacloud\utilities\keystore-explorer.sh` als Administrator oder mit Verwaltungsrechten aus.

Das Dienstprogramm verfügt über ein Onlinehilfesystem, in dem Sie Anleitungen zur Benutzeroberfläche erhalten.

- Java Keytool – Das Java Key and Certificate Management Tool verwaltet einen Keystore von Kryptografieschlüsseln, X.509-Zertifikatsketten und vertrauenswürdigen Zertifikaten. Es verwendet eine Befehlszeilenschnittstelle. Die Dokumentation zum Java Key and Certificate Management Tool ist für Unix- und Windows-Plattformen verfügbar:
  - Unix
  - Windows

3.9.4 Vorgehensweisen für verschiedene Aufgaben

Digitales Identitätszertifikat (Zertifizierungsantrag) beantragen

Verwendete Begriffe:

- Privater Schlüssel: Ein geheimer, nur dem Eigentümer bekannter Schlüssel, der zusammen mit einem Algorithmus der Ver- und Entschlüsselung von Daten dient
- Schlüsselpaar: der private Schlüssel und die zugehörige Zertifikatskette
- Eindeutiger Name: Die kenntlich machende Information in einem Zertifikat. Ein Zertifikat enthält den eindeutigen Namen zur Identifikation des Eigentümers/Requesters des Zertifikats und den eindeutigen Namen zur Identifikation des Zertifikatsausstellers.
- X.509-Zertifikat: ein digitales Zertifikat gemäß dem weithin akzeptierten internationalen X.509-Standard für PKI (Public Key Infrastructure; Infrastruktur für öffentliche Schlüssel), das dazu dient, die Eigentümerschaft des Benutzers am öffentlichen Schlüssel zu bestätigen

Vor dem Erstellen des Zertifizierungsantrags generiert der Antragsteller zuerst ein Schlüsselpaar und behält dabei den privaten Schlüssel geheim. Der Zertifizierungsantrag enthält Informationen, die den Antragsteller identifizieren (beispielsweise bei einem X.509-Zertifikat den eindeutigen Namen) und mit dem privaten Schlüssel des Antragstellers signiert werden müssen. Der Zertifizierungsantrag enthält außerdem den vom Antragsteller gewählten öffentlichen Schlüssel.

SO ERSTELLEN SIE EINEN ZERTIFIZIERUNGSANTRAG MIT KEYSTORE EXPLORER

Zum Erstellen einer Zertifikatsignieranforderung erstellen Sie ein Schlüsselpaar und generieren dann eine Zertifikatanforderung. Wenn Sie die Zertifikatinformationen nicht aktualisieren möchten,

können Sie den Schritt zum Erstellen des Schlüsselpaars überspringen und mit dem Generieren der Zertifikatanforderung fortfahren.

- Neues Schlüsselpaar erstellen

  a. Wählen Sie im Menü „Tools“ die Option „Generate Key Pair“ (Schlüsselpaar generieren) aus.

  b. Geben Sie im Dialogfeld „Generate Key Pair“ (Schlüsselpaar generieren) die Algorithmusinformationen und Zertifikatdetails ein. Klicken Sie auf „OK“.

  c. Geben Sie das entsprechende Alias (*servlet-engine*) und das standardmäßige Passwort (*changeit*) an.

- Zertifizierungsantrag generieren

  a. Wählen Sie das soeben erstellte Schlüsselpaar aus.

  b. Wählen Sie im Kontextmenü die Option „Generate CSR“ (Zertifizierungsantrag generieren) aus.

  c. Navigieren Sie zu dem Dateispeicherort, an dem Sie die Zertifikatsignieranforderung generieren möchten, und geben Sie den Dateinamen ein. Klicken Sie auf „OK“.

ZERTIFIZIERUNGSANTRAG MIT JAVA KEYTOOL ERSTELLEN

- Schlüsselpaar (Parameter `dname` mit eigenem Parameter ersetzen) im Ordner `sessionserver/etc` erstellen:

```
  ..\..\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
```

- Zertifizierungsantrag generieren:

```
  ..\..\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
```

  Nachdem Sie das Zertifikat von der Zertifizierungsstelle empfangen haben, importieren Sie es in Host Access for the Cloud.

Sitzungsserverzertifikat ersetzen

Die Installation wird mit eigensignierten Zertifikaten gesichert. Eigensignierte Zertifikate sind genauso sicher wie kommerzielle Zertifikate, werden aber nicht automatisch verbürgt. Deshalb ist ihre Verwaltung schwieriger. Kommerzielle Zertifikate sind erforderlich, wenn Sie eine breite Unterstützung für das Zertifikat benötigen. Die meisten Webbrowser und Betriebssysteme unterstützen bereits viele kommerzielle Zertifizierungsstellen.

Wichtige Informationen:

- Keystore-Speicherort: `/etc/keystore.bcfks`
- Keystore-Format: `bcfks` (Bouncy Castle FIPS)
- Standardmäßiges Passwort: *changeit*
- Schlüsselpaaralias: *servlet-engine*

Wie das eigensignierte Zertifikat ersetzt wird, hängt davon ab, ob Sie es im standardmäßigen Keystore durch ein Zertifikat ersetzen, das über einen Zertifizierungsantrag erhalten wurde, oder durch einen eigenen, nicht standardmäßigen Keystore mit Zertifikat.

Weitere Informationen

- Eigensigniertes Zertifikat mit der Zertifikatantwort der Zertifizierungsstelle (ZS) ersetzen
- Zertifikat mit nicht standardmäßigem Keystore ersetzen

Eigensigniertes Zertifikat mit der Zertifikatantwort der Zertifizierungsstelle ersetzen

1. Erstellen Sie einen Zertifizierungsantrag für den Sitzungsserver und senden Sie ihn an die Zertifizierungsstelle (ZS) Ihrer Wahl. Nach dem Empfang des signierten Zertifikats von der Zertifizierungsstelle gehen Sie wie folgt vor:
2. Importieren Sie das ZS-signierte Zertifkat bzw. die Zertifikatskette in den Keystore des Sitzungsservers.

   Sie können diese Aufgabe mit KeyStore Explorer oder mit den Java Keytool-Befehlszeilenanweisungen ausführen. Wenn die Antwort der Zertifizierungsstelle separate Dateien für das Stammzertifikat und das Zwischenzertifikat enthält, importieren Sie unabhängig vom verwendeten Werkzeug zunächst das Stammzertifikat und anschließend das Zwischenzertifikat in den Keystore.

   Verwenden von KeyStore Explorer

   a. Öffnen Sie `keystore.bcfks` in KeyStore Explorer. Verwenden Sie das Passwort *changeit*.

   b. Wenn separate Dateien für das Stammzertifikat und das Zwischenzertifikat verfügbar sind, wählen Sie in der Symbolleiste die Option „Import Trusted Certificate“ (Verbürgtes Zertifikat importieren) aus, um die Zertifikate zu importieren.

   c. Wählen Sie das Schlüsselpaar „servlet-engine“ aus. Klicken Sie mit der rechten Maustaste und wählen Sie „Import CA Reply“ (Antwort der Zertifizierungsstelle importieren) aus, um die Datei in das Schlüsselpaar zu importieren.

   d. Geben Sie bei der entsprechenden Aufforderung das Passwort *changeit* ein.

   e. Navigieren Sie zu dem Speicherort, an dem die Datei mit der Antwort der Zertifizierungsstelle gespeichert ist, wählen Sie die Datei aus, und klicken Sie auf „Importieren“.

   Verwenden von Java Keytool

   In den folgenden Beispielen werden Keytool-Befehle im Verzeichnis `sessionserver/etc` verwendet.

   Für Windows:

   Stammzertifizierungsstellenzertifikat und Zwischenzertifikat importieren

```
   ..\..\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
```

Antwort der Zertifizierungsstelle importieren

```
   ..\..\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
```

Für Unix:

Stammzertifizierungsstellenzertifikat und Zwischenzertifikat importieren

```
   ../../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.BouncyCastleFipsProvider

   ../../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.BouncyCastleFipsProvider
```

Antwort der Zertifizierungsstelle importieren

```
   ../../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.BouncyCastleFipsProvider
```

1. Verbürgen Sie das neue Zertifikat in MSS.

- Melden Sie sich als Administrator bei MSS an.
- Klicken Sie im linken Bereich auf „Configure Settings > Trusted Certificates“ (Einstellungen konfigurieren > Verbürgte Zertifikate).
- Wählen Sie „Trusted Sub-System“ (Verbürgtes Subsystem) aus. Die Liste enthält die von MSS verbürgten Zertifikate.
- Klicken Sie auf „IMPORT“ (Importieren), um das Sitzungsserverzertifikat zur Liste hinzuzufügen.
- Es ist nicht erforderlich, die Prozedur für jede MSS-Instanz zu wiederholen. Die Änderungen werden automatisch auf den anderen MSS-Instanzen im Cluster repliziert.

Eine ausführliche Hilfe ist in der Verwaltungskonsolenhilfe unter Trusted Certificates (Verbürgte Zertifikate) verfügbar.

Zertifikat mit nicht standardmäßigem Keystore ersetzen

Sie können einen anderen als den standardmäßigen Keystore (`sessionserver/etc/keystore.bcfks`) verwenden, um die ZS-signierten Zertifikate zu speichern.

Legen Sie in der Datei `sessionserver/conf/container.properties` die folgenden Eigenschaften fest:

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

Dabei wird der Keystore-Pfad auf den Dateinamen des nicht standardmäßigen Keystore gesetzt und das Keystore-Passwort auf den verschleierten Wert, der mit dem folgenden Befehl im Verzeichnis `sessionserver` generiert wird:

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

Beispiel:

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

> **Tipp**
>
> Löschen Sie den standardmäßigen Keystore, um Verwechslungen zu vermeiden.

Um zu verhindern, dass beim Starten des Servers der standardmäßige Keystore generiert wird, öffnen Sie `/conf/product-core-ctx.xml` in einem Texteditor und entfernen Sie den Abschnitt *servletEngineKeystoreGenerator* oder kommentieren Sie ihn aus. Starten Sie den Sitzungsserver neu.

MSS-Zertifikat ersetzen

 Lesen Sie die Informationen zum Ersetzen des MSS-Zertifikats im Thema General Security and Certificates (Allgemeine Sicherheit und Zertifikate).

Während der Installation hat der Sitzungsserver zum Herstellen einer sicheren Kommunikation das vorhandene MSS-Zertifikat verbürgt. Wenn das MSS-Zertifikat aktualisiert wird, muss es von allen HACloud-Sitzungsservern neu verbürgt werden.

So ersetzen Sie das MSS-Zertifikat:

- Um das neue MSS-Zertifikat zu verbürgen, importieren Sie es mit dem Alias „mss“ in den Truststore des Sitzungsservers (siehe Zertifikat in den Truststore des Sitzungsservers importieren).
- Sie müssen das neue MSS-Zertifikat in jeden Sitzungsserver importieren.

Sichere Emulationsverbindung zu einem verbürgten Host herstellen

Führen Sie die nachstehenden Schritte zum Konfigurieren einer TLS-Verbindung zwischen dem Host Access for the Cloud-Sitzungsserver und einem Host aus, der TLS unterstützt:

1. Konfigurieren Sie den vertrauenswürdigen Keystore in MSS.
2. Konfigurieren Sie die Terminalsitzung.

SO KONFIGURIEREN SIE DEN KEYSTORE IN MSS

Öffnen Sie die MSS-Verwaltungskonsole und wählen Sie „Configure Settings > Trusted Certificates“ (Einstellungen konfigurieren > Verbürgte Zertifikate) aus. Wählen Sie dann „Terminal Emulator Clients“ (Terminalemulatorclients). Sie können auf die Dokumentation für die Verwaltungskonsole zugreifen, indem Sie oben rechts auf der Seite auf das Hilfesymbol klicken.

Damit eine Sitzung den TLS-Host bei einem Verbindungsaufbau verbürgt, muss das öffentliche Zertifikat des Hosts mithilfe von Management and Security Server (MSS) zu einem verbürgten Keystore hinzugefügt werden. Die Host Access for the Cloud-Sitzung ruft dieses Zertifikat bei der ersten Verbindung einer Sitzung ab.

Wenn das Zertifikat zum verbürgten Keystore des MSS-Servers hinzugefügt wurde, kehren Sie zur Liste der Zertifikate zurück und sehen den neuen Host.

SO KONFIGURIEREN SIE EINE HACLOUD-TERMINALSITZUNG

Abhängig vom Hosttyp können Sie eine Terminalsitzung mit unterschiedlichen Sicherheitsprotokollen konfigurieren.

Typ	Prozedur
Unter Verwendung von TLS	Um eine Verbindung mit dem neuen verbürgten Host mit TLS herzustellen, konfigurieren Sie wie gewohnt eine Terminalsitzung und legen Sie im Dialogfeld der Einstellungen TLS als Sicherheitsprotokoll fest. Achten Sie darauf, für die Verbindung den richtigen TLS-Port anzugeben.
Verwenden von Secure Shell (SSH) mit VT-Hosttypen	Secure Shell bietet verschlüsselte Kommunikation zwischen dem Client und einem VT-Host. MSS enthält eine Liste der bekannten Hosts mit den öffentlichen Schlüsseln der Hosts, mit denen Sie sich über SSH verbinden können. SSH-Verbindungen können nur mit Hosts hergestellt werden, die bereits von einem Administrator als vertrauenswürdig eingestuft wurden. Bei der ersten Herstellung einer SSH-Verbindung zwischen einer Sitzung und einem Host wird die Datei mit den bekannten Hosts von MSS zum Sitzungsserver heruntergeladen. Wenn Sie versuchen, über SSH eine Sitzung im Bereich für die Sitzungsverwaltung zu erstellen oder zu bearbeiten, erhalten Sie eine Benachrichtigung, sofern der Schlüssel nicht als vertrauenswürdig anerkannt wird. Sie werden gefragt, ob Sie den Schlüssel als vertrauenswürdig einstufen und fortfahren möchten. • Wenn Sie „Ja“ eingeben, wird der Host verbürgt und zur Liste der bekannten Hosts hinzugefügt und Sie werden aufgefordert, das SSH-Hostpasswort einzugeben. • Wenn Sie nicht Ja eingeben, wird der Host weiterhin als nicht vertrauenswürdig eingestuft, und die Sitzung wird getrennt. Sie können die SSH-Datei mit den bekannten Hosts auch manuell konfigurieren, indem Sie eine SSH-Verbindung zwischen einer Sitzung und dem Host herstellen und den Schlüsselfingerabdruck des Remotehosts zur Liste der bekannten Hosts in MSS hinzufügen.
Konfigurieren der Datei der bekannten Hosts für SSH-Verbindungen in MSS	

1. Suchen Sie die Datei mit dem öffentlichen Schlüssel auf dem neuen SSH-Host, z. B. `/etc/ssh/ssh_host_rsa_key.pub`. Die einzigen gültigen Arten öffentlicher Schlüssel für known_hosts-Einträge in MSS sind `ssh-rsa` und `ssh-dss`. Mögliche Formate für öffentliche Schlüssel des Hosts sind OpenSSH, Base64-encode, DER oder PFX. Die Datei muss diesem Format entsprechen: Hostname, IP-Adresse, Schlüsselart, Schlüssel. Der öffentliche Schlüssel kann beispielsweise so aussehen: `alpsuse132, 10.117.16.232 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA.....`
2. Melden Sie sich bei MSS an (z. B. über `http://mycompany.com/adminconsole`).
3. Öffnen Sie die Verwaltungskonsole.
4. Klicken Sie auf „Einstellungen konfigurieren > Secure Shell“ und importieren Sie den öffentlichen Schlüssel. Nachdem der öffentliche Schlüssel in die Datei der bekannten Hosts importiert wurde, kehren Sie zur Seite „Secure Shell Known Hosts“ (Bekannte Secure Shell-Hosts) zurück und der neue Host wird in der Liste angezeigt.
5. Befolgen Sie die Anweisungen in MSS zum Importieren eines bekannten Hosts. Nachdem der öffentliche Schlüssel in die Datei der bekannten Hosts importiert wurde, kehren Sie zur Seite „Secure Shell Known Hosts“ (Bekannte Secure Shell-Hosts) zurück und der neue Host wird in der Liste angezeigt.

Serverseitige Ereignissen zum Ausführen von ausgehenden TLS-Aufrufen vom Sitzungsserver einrichten

Beim Verfassen von Java-Code, der in den serverseitigen Ereignissen ausgeführt wird, möchten Sie möglicherweise ausgehende Aufrufe an Remoteserver mit TLS ausführen. Wenn der Remoteserver bekannt ist, ist er möglicherweise bereits vom Sitzungsserver verbürgt und es ist keine weitere Einrichtung erforderlich. Oft ist der Remoteserver jedoch nicht bekannt und muss durch Importieren des Zertifikats in den Truststore des Sitzungsservers verbürgt werden.

So verbürgen Sie den Remoteserver:

Importieren Sie das öffentliche Zertifikat des Remoteservers in den Truststore des Sitzungsservers. Befolgen Sie dazu die Anweisungen unter Zertifikat in den Truststore des Sitzungsservers importieren.

Weitere MSS-Server zur Installation hinzufügen

Während der Installation haben die MSS- und HACloud-Server ihre Zertifikate ausgetauscht und verbürgt. Wenn Sie weitere MSS-Server hinzufügen, müssen deren Zertifikate ebenfalls verbürgt werden.

MSS Eine Konfiguration ist in der MSS-Verwaltungskonsole unter „Configure Settings > Trusted Certificates > Trusted Sub-System“ (Einstellungen konfigurieren > Verbürgte Zertifikate > Verbürgtes Subsystem) erforderlich.

SO RICHTEN SIE DIE VERBÜRGUNG ZWISCHEN MSS UND DEN SITZUNGSSERVERN EIN

- Verbürgen Sie den neuen MSS-Server, indem Sie das MSS-Zertifikat in den Truststore des Sitzungsservers importieren (siehe Zertifikat in den Truststore des Sitzungsservers importieren).
- Der neue MSS-Server muss jeden Sitzungsserver verbürgen.
  a. Melden Sie sich als Administrator bei MSS an.
  b. Klicken Sie im linken Bereich auf „Configure Settings > Trusted Certificates“ (Einstellungen konfigurieren > Verbürgte Zertifikate).
  c. Wählen Sie „Trusted Sub-System“ (Verbürgtes Subsystem) aus. Die Liste enthält die von MSS verbürgten Zertifikate.
  d. Klicken Sie auf „Import“ (Importieren), um das Sitzungsserverzertifikat zur Liste hinzuzufügen.
  e. Wiederholen Sie diesen Vorgang für jeden Sitzungsserver.

Zusätzliche Sitzungsserver zu einer Installation mit mehreren MSS-Servern hinzufügen

Während der Installation haben der Sitzungsserver und MSS bereits ihre Zertifikate ausgetauscht und verbürgt. Alle MSS-Server verbürgen bereits alle vorhandenen Sitzungsserver. Wenn Sie jedoch weitere Sitzungsserver hinzufügen, muss zwischen dem neuen Sitzungsserver und den vorhandenen MSS-Servern eine Verbürgungsbeziehung hergestellt werden..

SO FÜGEN SIE WEITERE SITZUNGSSERVER HINZU:

1. Importieren Sie das MSS-Serverzertifikat in den Sitzungsserver-Truststore.
2. Importieren Sie das Sitzungsserverzertifikat in den Truststore des MSS-Servers. Weitere Informationen hierzu finden Sie unter „General Security and Certificates“ (Allgemeine Sicherheit und Zertifikate) in der MSS-Dokumentation.
3. Rufen Sie `service.registry.password` aus der Datei `container.properties` vom MSS-Server ab.
4. Legen Sie `service.registry.password` in der Datei `container.properties` auf dem Sitzungsserver fest.

Weitere Informationen

- Zertifikat in den Truststore des Sitzungsservers importieren
- General Security and Certificates (Allgemeine Sicherheit und Zertifikate) in der MSS-Dokumentation

Zertifikat in den Truststore des Sitzungsservers importieren

Wenn der Sitzungsserver versucht, ausgehende sichere Verbindungen zu Remoteservern herzustellen, überprüft er die Identität des Remoteservers mithilfe der Zertifikate in seinem Truststore. Jedes in den Truststore importierte Zertifikat wird verbürgt.

Wichtige Informationen:

- Keystore-Speicherort: `/etc/trustcerts.bcfks`
- Keystore-Format: `bcfks` (Bouncy Castle FIPS)
- Standardmäßiges Passwort: *changeit*

MIT KEYSTORE EXPLORER

1. Öffnen Sie `trustcerts.bcfks` unter Verwendung des Passworts *changeit*.
2. Wählen Sie in der Symbolleiste die Option „Import Trusted Certificate“ (Verbürgtes Zertifikat importieren) aus.

MIT JAVA KEYTOOL

Im Verzeichnis `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
```

3.10 Verwenden von Docker

Für die offene Docker-Plattform steht eine hervorragende Dokumentation zur Verfügung, die Sie lesen und beachten sollten.

3.10.1 Warum Docker?

Docker ist eine eigenständige Plattform, mit der Sie Anwendungen in einem Container entwickeln, bereitstellen und ausführen können. Ihre Anwendung, alle von der Anwendung benötigten Abhängigkeiten, wie Binärdateien und Bibliotheken, und die Konfigurationsinformationen sind im Container enthalten. Sie können mehrere Container bereitstellen, die alle in Docker und über dem Betriebssystem ausgeführt werden.

Mithilfe von Docker können Sie Ihre Anwendungen vertikal skalieren, d. h. mehrere Instanzen des Sitzungsservers können auf einem Server vorhanden sein und jede Instanz liefert die gleiche Leistung, die sie beim Erstellen und Testen bot.

3.10.2 Welche Vorteile bietet dies?

Die Verwendung von Containern bietet mehrere Vorteile:

- Leistung

  Virtuelle Maschinen sind eine Alternative zu Containern. Container enthalten jedoch (im Gegensatz zu virtuellen Maschinen) kein Betriebssystem. Das bedeutet, dass Container schneller erstellt und gestartet werden können und einen kleineren Fußabdruck hinterlassen.

- Agilität

  Weil Container portabler sind und eine bessere Leistung bieten, können Sie agilere und dynamische Entwicklungsmethoden nutzen.

- Isolation

  Docker-Container sind unabhängig voneinander. Dies bietet den Vorteil, dass ein Docker-Container, der eine Anwendung und die erforderlichen Versionen der unterstützenden Software enthält, nicht mit einem anderen Container mit der gleichen Anwendung, aber anderer unterstützender Software, in Konflikt geraten kann. So können Sie sicher sein, dass sich das Image, das Sie erstellen, in jeder Entwicklungs- und Bereitstellungsphase genau wie erwartet verhält.

- Skalierbarkeit

  Neue Container lassen sich einfach und schnell erstellen. Die Docker-Dokumentation enthält Informationen zum Verwalten mehrerer Container.

3.10.3 Terminologie

Zum Arbeiten mit Docker sollten Sie mit einigen Grundbegriffen vertraut sein. Weitere Information finden Sie auf der Website zur Docker-Dokumentation.

Container

Eine Laufzeitinstanz eines Image. Ein Container ist üblicherweise vollständig von der Hostumgebung isoliert und kann nur auf Hostdateien und -ports zugreifen, wenn er entsprechend konfiguriert wurde. Um ein Image in einem Container auszuführen, verwenden Sie den Docker-Befehl „run“.

Docker Hub

Eine Cloud-basierte Community-Ressource für das Arbeiten mit Docker. Docker Hub dient üblicherweise dem Hosten von Images, kann aber auch für die Benutzerauthentifizierung und Automatisierung der Image-Erstellung verwendet werden. Jeder kann Images in Docker Hub veröffentlichen.

Docker Compose

Compose ist ein Werkzeug, das mithilfe von YAML-Dateien Ihre Anwendungsservices konfiguriert und dann Docker-Anwendungen mit mehreren Containern definiert und ausführt. Weitere Informationen zu Compose finden Sie in der Docker Compose-Dokumentation.

Dockerfile

Ein Textdokument, das die Befehle zum Erstellen eines Docker-Image enthält. Sie können komplexe Befehle (zum Beispiel zum Festlegen eines vorhandenen Image als Basis) oder einfache Befehle (zum Beispiel zum Kopieren von Dateien zwischen Verzeichnissen) angeben. Um ein Image von einer Dockerfile-Datei zu erstellen, verwenden Sie den Docker-Befehl „build“.

Image

Ein eigenständiges, ausführbares Paket, das in einem Container ausgeführt wird. Ein Docker-Image ist eine Binärdatei, die alle erforderlichen Elemente zum Ausführen eines einzelnen Docker-Containers einschließlich Metadaten enthält. Sie können eigene Images (mit einer Dockerfile-Datei) erstellen oder Images verwenden, die von anderen Personen erstellt und in einer Registrierung (wie Docker Hub) verfügbar gemacht wurden. Um ein Image von einer Dockerfile-Datei zu erstellen, verwenden Sie den Docker-Befehl „build“. Um ein Image in einem Container auszuführen, verwenden Sie den Docker-Befehl „run“.

3.10.4 Erste Schritte mit Docker und Host Access for the Cloud

Wenn Sie sich bei der Installation von HACloud für die Verwendung von Docker entscheiden, enthält das Installationspaket eine anfängliche Dockerfile und eine zugehörige JAR-Anwendungsdatei für die ersten Schritte bei der Verwendung des Sitzungsservers in Containern. Diese Dateien sind vor der Installation verfügbar.

> **Hinweis**
>
> Stellen Sie sicher, dass Sie die neueste Version von Docker und Docker Compose ausführen.

Der Ordner `docker/samples` enthält Beispiele. Weitere Anleitungen dazu finden Sie unter Beispiele.

Das Erstellen des Basisimage erfolgt in vier Schritten:

1. Docker installieren. Befolgen Sie die Anweisungen auf der Docker-Website.
2. Extrahieren Sie die Downloadpaketdatei und suchen Sie die Dateien `Dockerfile`, `entrypoint.sh` und `sessionserver.jar` im Docker-Ordner. Für die Datei `entrypoint.sh` muss das ausführbare Bit festgelegt sein.
3. Erstellen Sie das Docker-Image.
4. Führen Sie das Docker-Image aus.

Docker-Image erstellen

Nachdem Sie den ersten und zweiten Schritt ausgeführt haben, d. h. Docker installiert und die Dockerfile und die sessionserver.jar-Datei extrahiert und gefunden haben, besteht der nächste Schritt im Erstellen des Docker-Basisimage des Sitzungsservers.

1. Führen Sie im Ordner, der die Dockerfile enthält, den folgenden Befehl aus:

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

   Ersetzen Sie `<Version>` mit der Version des Sitzungsservers. Wenn keine Version verfügbar ist, ist das Standard-Tag `(-t) latest` (neueste Version).
2. Überprüfen Sie, ob das Image erfolgreich erstellt wurde. Führen Sie den folgenden Befehl aus:

   ```
   docker images
   ```

   Die Ausgabe sollte Informationen zum soeben erstellten Image enthalten.

Image ausführen

Bevor Sie das Image des Sitzungsservers in einem Docker-Container ausführen können, müssen Sie diese Schritte ausführen:

- **Adresse des MSS-Servers angeben**

  Um den Ort des MSS-Servers anzugeben, übergeben Sie eine Umgebungsvariable über Docker an den Sitzungsserver. Beispiel: `--env MSS_SERVER=mss.server.com`

- **Passwort für Serviceregistrierung angeben**

  Um das Passwort für die Serviceregistrierung anzugeben, übergeben Sie eine Umgebungsvariable über Docker an den Sitzungsserver. Beispiel: `--env SERVICE_REGISTRY_PASSWORD=<Ihr_Passwort> .`

  Das Passwort ist in der Eigenschaft `service.registry.password` unter . `/mss/server/conf/container.properties` auf dem MSS-Server abrufbar. Verwenden Sie die gesamte Eigenschaft `service.registry.password` .

- **MSS anweisen, dem Identitätszertifikat des Sitzungsservers zu vertrauen**

  Führen Sie diesen Schritt in der Verwaltungskonsole unter „Configure Settings > Trusted Certificates“ (Einstellungen konfigurieren > Verbürgte Zertifikate) aus. Weitere Informationen finden Sie in der Dokumentation zur MSS-Verwaltungskonsole unter Trusted Certificates (Verbürgte Zertifikate/). Das Zertifikat des Sitzungsservers ist im Verzeichnis sessionserver/etc verfügbar.

- **Keystore mit dem Identitätszertifikat des Sitzungsservers angeben**

  Der Sitzungsserver weist sich mithilfe eines Zertifikats aus. Dieses Zertifikat sollte im Java-Keystore `/sessionserver/etc/keystore.bcfks` im Container hinterlegt sein. Der Schlüsselpaareintrag servlet-engine muss die vollständige Zertifikatskette enthalten.

- **Truststore mit MSS-Zertifikat angeben**

  Wenn der Sitzungsserver ausgehende TLS-Verbindungen aufbaut, prüft er die Vertrauenswürdigkeit der Remoteserver (z. B. MSS) anhand der Zertifikate in seinem Truststore. Zertifikaten, die sich im Java-Keystore `/sessionserver/etc/trustcerts.bcfks` des Containers befinden, wird vertraut.

- **Keystore und Truststore zu denen im Container zuordnen**

  Sie können dem Container die Keystores auf zwei Wegen präsentieren:

  - Per Volume-Mount

    Alternativ:

  - Vorhandenes Docker-Image erweitern

Per Volume-Mount

Mit einem Volume-Mount wird eine Datei oder ein Verzeichnis auf dem Hostcomputer im Container eingehängt. Die Datei bzw. das Verzeichnis wird mit dem vollständigen oder relativen Pfad auf dem Hostcomputer referenziert.

Mit dem Volume-Mount werden die Keystore- und Truststore-Dateien auf dem Host im Docker-Container eingehängt.

```
docker run -d \
--env MSS_SERVER=<MSS-Servername> \
--env SERVICE_REGISTRY_PASSWORD=<Passwort hier eingeben> \
--env MANAGEMENT_SERVER_URL=https://<MSS-Servername>:<Port>/mss \
--env HOST_NAME=<DNS-Name_des_Docker-Servers> \
--volume ~/demo_keystore.bcfks:/sessionserver/etc/keystore.bcfks \
--volume ~/demo_truststore.bcfks:/sessionserver/etc/trustcerts.bcfks \
--publish 7443:7443 \
sessionserver
```

Vorhandenes Docker-Image erweitern

Mit dieser Methode erstellen Sie eine neue Dockerfile-Datei, um die erforderlichen Dateien in das Docker-Image zu kopieren. Auf diese Weise lässt sich das Docker-Image besser verschieben.

- Erstellen Sie zuerst eine Dockerfile, die aus dem Docker-Image `hacloud/sessionserver` erweitert wird.
- VON hacloud/sessionserver: `<Beispiel: hacloud/sessionserver:latest oder hacloud/sessionserver:version>`
- KOPIEREN SIE: `<Ihr-Pfad>/keystore.bcfks /sessionserver/etc/keystore.bcfks`
- KOPIEREN SIE: `<Ihr-Pfad>/truststore.bcfks /sessionserver/etc/trustcerts.bcfks`
- Erstellen Sie dann das erweiterte Docker-Image und nennen Sie es „demo“.

  `docker build -t demo .`
- Führen Sie dann das Image „demo“ aus.

```
docker run -d \
--env MSS_SERVER=<MSS-Servername> \
--env SERVICE_REGISTRY_PASSWORD=<Passwort hier eingeben> \
--env MANAGEMENT_SERVER_URL=https://<MSS-Servername>:<Port>/mss \
--env HOST_NAME=<DNS-Name_des_Docker-Servers> \
--publish 7443:7443 \
demo
```

- **Docker-Hostname und -Port angeben**

  Damit MSS den Sitzungsserver findet, muss dieser seinen Hostnamen versenden. Da Docker einen zufälligen einmaligen Namen generiert, der von außerhalb des Containers nicht erreichbar ist, müssen Sie den Docker-Hostnamen für MSS angeben. Teilen Sie dem Sitzungsserver außerdem mit, welchen Port Sie auf Ihrem Docker-Host veröffentlichen. Clients, die auf den Sitzungsserver zugreifen, werden hier herauskommen: `<Docker_Hostname>:<Docker_veröffentlichter_Port>`.

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

3.10.5 Beispiele

Die Beispiele im Ordner „docker/samples“ illustrieren vier Szenarien mit Docker Compose. Compose ist ein Werkzeug, das eine YAML-Datei verwendet, um die Anwendungen mit einem einzigen Befehl zu konfigurieren und auszuführen.

Voraussetzungen

So führen Sie die Beispiele aus:

- Installieren Sie Docker Compose. Machen Sie sich vor dem Fortfahren mit der Docker-Dokumentation zu Docker Compose vertraut.
- Sie benötigen einen MSS-Server, der ausgeführt wird.
- Sie benötigen eine Keystore-Datei zum Sichern von TLS-Verbindungen zum Sitzungsserver, der MSS vertraut.
- Sie benötigen eine Truststore-Datei mit eingerichtetem MSS-Serverzertifikat.
- Erstellen Sie das Docker-Image für den Sitzungsserver.

Folgende Beispiele sind verfügbar:

- Einfaches Beispiel: Ein einfaches Beispiel mit Demo-Keystore- und Demo-Truststore-Dateien, in die Sie ein MSS-Serverzertifikat importieren können.
- Hybrid: Ein Beispiel eines Hybridszenarios mit einer lokalen Host Access for the Cloud-Installation, in dem auf einem Datenträger vorhandene Keystore- und Truststore-Dateien im Docker-Container eingehängt werden.
- Erweiterungen: Ein Beispiel mit einer Erweiterung, das darstellt, wie der Webclient aktualisiert, geändert und angepasst werden kann.
- Lastverteiler: Ein Beispiel mit Lastverteiler, das den Lastausgleich zwischen verknüpften Containern beschreibt.

Einfaches Beispiel

Dieses einfache Beispiel zeigt, wie das Docker-Image des Sitzungsservers in Docker Compose ausgeführt wird. Für dieses Beispiel müssen Sie das Zertifikat des MSS-Servers in das bereitgestellte Beispiel `./certs/demo_truststore.bcfks` importieren. Verwenden Sie dazu beispielsweise KeyStore Explorer. Standardmäßig befindet sich Ihr MSS-Zertifikat unter `/mss/server/etc/<Computername>.cer`. Siehe Zertifikat in den Truststore des Sitzungsservers importieren.

Bevor Sie das Beispiel ausführen, aktualisieren Sie die Werte MSS_SERVER, HOST_NAME und SERVICE_REGISTRY_PASSWORD in `docker-compose.yml`.

- So starten Sie den Sitzungsserverdienst:

  `docker-compose up`

- So führen Sie den Service in einem Daemon aus (getrennter Modus):

  `docker-compose up -d`

- So zeigen Sie ausgeführte Container an:

  `docker ps`

Beispiel eines Hybridszenarios

In diesem Beispiel ist eine lokale Installation von Host Access for the Cloud mit Keystore- und Truststore-Dateien auf einem Datenträger vorhanden. Diese Dateien müssen im Docker-Container eingehängt (dorthin kopiert) werden.

Bevor Sie das Beispiel ausführen, aktualisieren Sie die Werte MSS_SERVER, HOST_NAME, SERVER_PORT und SERVICE_REGISTRY_PASSWORD in der ENV-Datei.

So starten Sie den Sitzungsserverdienst:

- Kopieren Sie `.env` und `docker-compose.yml` zu `sessionserver/microservices/sessionserver/`.
- Führen Sie aus diesem Verzeichnis Folgendes aus: `docker-compose up -d`

Beispiel für ein Erweiterungsszenario

Mithilfe von Erweiterungen und eigenem HTML-, CSS- oder JavaScript-Code können Sie die Darstellung des Webclients über den Browser aktualisieren, ändern und anpassen. Weitere Informationen finden Sie unter „Erweitern des Webclients“.

In diesem Beispiel wird SPRING_PROFILES_ACTIVE auf „extensions_enabled“ festgelegt und der Speicherort der Erweiterungen in `docker-compose.yml` zugeordnet.

Bevor Sie das Beispiel ausführen, aktualisieren Sie die Werte MSS_SERVER, HOST_NAME, und SERVICE_REGISTRY_PASSWORD in der ENV-Datei.

So starten Sie den Sitzungsserverdienst:

`docker-compose up -d`

Sie könnten außerdem das Docker-Basisimage „hacloud/sessionserver“ erweitern und die Erweiterungsdateien in den Docker-Container kopieren:

1. Erstellen Sie die Dockerfile, die aus dem Docker-Image „hacloud/sessionserver“ erweitert wird.

```
FROM hacloud/sessionserver

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

2. Erstellen Sie das erweiterte Docker-Image und nennen Sie es *extensions*.

```
docker build -t extensions .
```

3. Aktualisieren Sie `docker-compose.yml` zur Verwendung des neuen Image „extensions“.

```
version: '3'
services:
  sessionserver:
    image: extensions
    environment:
        - LOGGING_FILE_NAME=./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
```

Lastausgleich

HAProxy ist ein Lastverteiler. Weitere Informationen zu HAProxy erhalten Sie auf der zugehörigen Website.

In diesem Beispiel wird ein haproxy-Service in die Datei `docker-compose.yml` eingeschlossen. Das Beispiel verwendet ein haproxy-Image zum Ausgleich zwischen verknüpften Containern. Dieses Beispiel verwendet SLL-Bridging zum Verknüpfen der Container.

Um eine sichere Kommunikation zwischen den Clients und dem Lastverteiler zu gewährleisten, aktualisieren Sie die Eigenschaft `LOAD_BALANCER_CERT` in der `.env` -Datei mit dem Speicherort des Lastverteilerzertifikats.

Zum Testen können Sie ein eigensigniertes Zertifikat generieren:

1. Generieren Sie einen eindeutigen privaten Schlüssel (KEY):

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

2. Generieren Sie einen Zertifizierungsantrag (CSR):

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

3. Erstellen Sie ein eigensigniertes Zertifikat (CRT):

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

4. Fügen Sie KEY und CERT an loadbalancer-pem an:

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

So starten Sie die Sitzungsserver- und haproxy-Services:

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

Alternativ:

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

Hierbei stellt „n“ die Anzahl der Sitzungsserverinstanzen dar.

Sie können die Anzahl der Sitzungsserverinstanzen nach dem Starten des Services ändern:

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

So greifen Sie auf den Sitzungsserver und die HAProxy-Statistikseite zu:

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

Verwenden Sie:

- Benutzer: *admin*
- Passwort: *password*

4. Verwalten

4.1 Verwalten

Durch das Erstellen und Konfigurieren von Sitzungen und Sicherstellen des störungsfreien und sicheren Betriebs schaffen Sie optimale Bedingungen für Ihre Benutzer. Mit den folgenden Vorgängen können Sie Ihre Host Access for the Cloud-Sitzungen und -Hostverbindungen organisieren und verwalten.

- Erstellen von Hostsitzungen
- Bereitstellen von Zugriff auf Hostsitzungen
- Verwalten der Benutzereinstellungen
- Anpassen von Hostsitzungen
- Protokollierung

4.2 Erstellen von Hostsitzungen

Host Access for the Cloud unterstützt IBM 3270-, 5250- und VT-Hosts und die Hosttypen UTS, T27 und ALC.

Ihre Benutzer können über von Ihnen erstellte und konfigurierte Sitzungen auf den Host zugreifen. Sitzungen werden von einem Administrator in der MSS-Verwaltungskonsole erstellt. Wenn Sie über die Verwaltungskonsole eine Sitzung starten, wird in einem separaten Browserfenster der Bereich „Verbindung“ des Webclients geöffnet. In diesem Bereich konfigurieren Sie die Verbindungsoptionen. Die Optionen können abhängig vom Hosttyp voneinander abweichen.

So erstellen Sie eine Sitzung:

1. Erstellen Sie Sitzungen in der MSS-Verwaltungskonsole. Weitere Informationen finden Sie unter Add a Session (Sitzung hinzufügen) in der MSS-Dokumentation.
2. Wählen Sie im HACloud-Webclient im Dialogfeld **Neue Sitzung erstellen** in der Dropdown-Liste die Art des Hosts aus, zu dem Sie eine Verbindung herstellen.
3. Geben Sie im Bereich „Verbindung“ den Namen des Hosts ein, zu dem die Verbindung hergestellt werden soll. Sie können den vollständigen Hostnamen oder seine vollständige IP-Adresse angeben.
4. Geben Sie die Nummer des Ports ein, den Sie verwenden möchten.
5. Geben Sie die für die Hostverbindung benötigten Informationen ein.
6. Speichern Sie die Verbindungseinstellungen.
7. Klicken Sie nach dem Konfigurieren und Testen der Sitzung auf „Beenden“, um zur MSS-Verwaltungskonsole zurückzukehren.
8. Weisen Sie den Benutzern über die Ansicht Assign Access (Zugriff zuweisen) in der MSS-Verwaltungskonsole die Sitzung zu.
9. Sobald Ihren Benutzern Sitzungen zugewiesen wurden, können Sie sie darüber informieren, wie sie auf ihre Sitzungen zugreifen können.

Überprüfen Sie die Einstellungen für Ihren Sitzungstyp.

- Allgemeine Verbindungseinstellungen
- 3270- und 5250-Verbindungseinstellungen
- VT-Verbindungseinstellung
- UTS-Verbindungseinstellungen
- T27-Verbindungseinstellungen
- ALC-Verbindungseinstellungen

4.3 Verbindungseinstellungen

4.3.1 Verbindungseinstellungen

Host Access for the Cloud unterstützt IBM 3270-, 5250- und VT-Hosts und die Hosttypen UTS, T27 und ALC.

Ihre Benutzer können über von Ihnen erstellte und konfigurierte Sitzungen auf den Host zugreifen. Sie konfigurieren die Verbindungsoptionen über den Bereich „Einstellungen“. Es gibt eine Reihe von Einstellungen, die für alle Hosttypen gemeinsam gelten. Andere Optionen variieren je nach Hosttyp.

Weitere Informationen

- Allgemeine Verbindungseinstellungen
- 3270 und 5250
- VT
- UTS
- T27
- ALC

4.3.2 Allgemeine Verbindungseinstellungen

Diese Optionen gelten für alle unterstützten Hosttypen.

- **Beim Start verbinden**

  Sitzungen sind standardmäßig so konfiguriert, dass sie beim Erstellen oder Öffnen einer Sitzung automatisch eine Verbindung zum Host herstellen. Sie können jedoch auch eine Sitzung einrichten, die nicht automatisch eine Verbindung zum Host aufbaut. Wählen Sie „NEIN“, um eine manuelle Verbindung zum Host herzustellen.

- **Erneut verbinden, wenn der Host die Verbindung beendet**

  Wenn diese Option aktiviert ist, versucht Host Access for the Cloud eine neue Verbindung herzustellen, sobald die Hostverbindung beendet wird.

- **Protokoll**

  Wählen Sie aus der Dropdownliste das Protokoll aus, das für die Kommunikation mit dem Host verwendet werden soll. Um eine Hostverbindung herzustellen, müssen der Webclient und der Hostcomputer dasselbe Netzwerkprotokoll verwenden. Die verfügbaren Werte hängen von dem Host ab, mit dem Sie eine Verbindung herstellen. Dazu gehören:

Protokoll	Beschreibung
TN3270	TN3270 ist eine Form des Telnet-Protokolls. Dieses Protokoll definiert eine bestimmte Anzahl von Spezifikationen für die allgemeine Kommunikation zwischen Desktopcomputern und Hostsystemen. Es verwendet TCP/IP als Transportprotokoll zwischen Desktopcomputern und IBM-Mainframes.
TN3270E	TN3270E oder Telnet Erweitert ist für Benutzer von TCP/IP gedacht, die über ein Telnet-Gateway mit RFC 1647-Implementierung eine Verbindung zum IBM-Mainframe herstellen. Mit dem Protokoll TN3270E können Sie den Verbindungsgerätenamen (auch LU-Name genannt) angeben. Ferner verfügen Sie über Standardunterstützung für die Tasten ATTN und SYSREQ sowie die SNA-Antwortbehandlung. Wenn Sie mit Telnet Erweitert eine Verbindung zu einem Gateway aufbauen, das dieses Protokoll nicht unterstützt, wird stattdessen das Standardprotokoll TN3270 verwendet.
TN5250	TN5250 ist eine Form des Telnet-Protokolls. Dieses Protokoll definiert eine bestimmte Anzahl von Spezifikationen für die allgemeine Kommunikation zwischen Desktopcomputern und Hostsystemen. Es verwendet TCP/IP als Transportprotokoll zwischen Desktopcomputern und AS/400-Computern.
Secure Shell (VT)	Das Konfigurieren von SSH-Verbindungen empfiehlt sich zum Gewährleisten einer sicheren, verschlüsselten Kommunikation zwischen Ihrem Computer und einem zuverlässigen VT-Host über ein unsicheres Netzwerk. Mit SSH-Verbindungen wird neben der Authentifizierung von Clientbenutzer und Hostcomputer auch die Verschlüsselung aller Daten sichergestellt. Zwei Authentifizierungsoptionen stehen zur Verfügung: • **Interaktiv über die Tastatur** – Sie können diese Authentifizierungsmethode zum Implementieren verschiedener Arten von Authentifizierungsmechanismen verwenden. Jede aktuell unterstützte Authentifizierungsmethode, die nur die Eingabe des Benutzers erfordert, kann über „Interaktiv über die Tastatur“ ausgeführt werden. • **Passwort** – Mit dieser Option wird der Client zur Eingabe eines Passworts für den Host aufgefordert, nachdem eine Verbindung mit dem Host hergestellt wurde. Das Passwort wird dann durch den verschlüsselten Kanal an den Host weitergeleitet.
Telnet (VT)	Telnet ist ein Protokoll aus dem TCP/IP-Paket offener Protokolle. Als Zeichenstromprotokoll überträgt Telnet Benutzereingaben aus Zeichenmodus-Anwendungen zeichenweise über das Netzwerk an den Host, wo sie verarbeitet und als Echorückmeldungen über das Netz gesendet werden.

INT1 (UTS)	Ermöglicht den Zugriff auf Unisys 1100/1200-Hosts über das TCP/IP-Netzwerkprotokoll.
TCPA (T27)	Verwenden Sie dieses Protokoll für die Verbindung mit Hosts der Unisys ClearPath NX/LX Series oder der A Series. Bei der TCPA-Authentifizierung werden die Benutzeranmeldeinformationen überprüft. Bei der richtigen Konfiguration können Sie Sicherheitsanmeldeinformationen vom Anmeldeinformationsserver Ihrer Anwendung anfordern und die Anmeldeinformationen zurück an den Server senden. Wenn der Berechtigungsnachweis gültig ist, wird die Anwendung angemeldet. Sie müssen dann keine Benutzer-ID und kein Passwort eingeben. Wenn der Berechtigungsnachweis jedoch nicht gültig ist, werden Sie zur Eingabe einer Benutzer-ID und eines Passworts aufgefordert.
MATIP (ALC)	Das MATIP-Protokoll (Mapping of Airline Traffic Over Internet Protocol) verwendet TCP/IP für Buchungen, Reservierungen und Airline-spezifischen Datenverkehr.

- **TLS-Sicherheit**

  Über TLS-Protokolle können Clients und Server sichere, verschlüsselte Verbindungen in einem öffentlichen Netzwerk herstellen. Wenn Sie mithilfe von TLS Verbindungen herstellen, authentifiziert Host Access for the Cloud den Server, bevor eine Sitzung geöffnet wird. Alle Daten, die zwischen Host Access for the Cloud und dem Host übertragen werden, werden mit der ausgewählten Verschlüsselungsstufe verschlüsselt.

  > **Tipp**
  >
  > Wenn „TLS-Sicherheit“ auf „TLS 1.3“ oder „TLS 1.2“ festgelegt ist, steht die Option zur Verfügung, den Hostnamen mit dem Namen im Serverzertifikat zu vergleichen. Es wird dringend empfohlen, die Überprüfung des Hostnamens für alle Sitzungen zu aktivieren.

  Folgende Optionen stehen zur Auswahl:

Sicherheitsoptionen	Beschreibung
Keine	Es ist keine sichere Verbindung erforderlich.
TLS 1.3	Mit TLS 1.3 verbinden. Wenn **Serveridentität überprüfen** auf **Ja** festgelegt ist, vergleicht der Client den Server- oder Hostnamen mit dem Namen im Serverzertifikat. Es wird dringend empfohlen, die Überprüfung des Hostnamens für alle Sitzungen zu aktivieren.
TLS 1.2	Mit TLS 1.2 verbinden. Wenn **Serveridentität überprüfen** auf **Ja** festgelegt ist, vergleicht der Client den Server- oder Hostnamen mit dem Namen im Serverzertifikat. Es wird dringend empfohlen, die Überprüfung des Hostnamens für alle Sitzungen zu aktivieren.

  > **Hinweis**
  >
  > Informationen zum Hinzufügen verbürgter Zertifikate, zu Schlüsselspeichern, zur Verwendung von SSH und weitere ausführliche Sicherheitsinformationen finden Sie im Abschnitt Sichere Verbindungen.

- **Emulationsverfolgung aktivieren**

  Sie können festlegen, dass Hostprotokolle für eine Sitzung generiert werden. Die Standardeinstellung ist „Nein“. Wählen Sie „Ja“ aus, damit bei jedem Start der Sitzung eine neue Trace-Datei für den Emulationshost erstellt wird. Die Trace-Datei wird unter `<Installationsverzeichnis>/sessionserver/logs/hosttraces/<Datum (jjjjmmtt>/<Trace-Datei>` gespeichert.

Terminal ID Manager verwenden

MSS Um Terminal ID Manager verwenden zu können, muss ein Terminal ID Manager-Server konfiguriert sein. Siehe Einrichten von Terminal ID Manager.

Wenn Sie **Terminal ID Manager** ausgewählt haben, können Sie damit Client-Anwendungen zur Laufzeit IDs bereitstellen und gepoolte IDs für verschiedene Hosttypen verwalten. Eine Kennung besteht aus Verbindungsdaten, die für eine einzelne Hostsitzung eindeutig sind.

Wenn Sie Terminal ID Management verwenden möchten und den Terminal ID Management-Server konfiguriert haben, können Sie anhand der nachstehenden Optionen die Kriterien zum Abrufen einer Kennung konfigurieren. Eine Kennung wird nur dann zurückgegeben, wenn alle angegebenen Kriterien erfüllt sind.

> **Hinweis**
>
> Beachten Sie, dass Sie durch Angabe eines Kriteriums festlegen, dass die Kennung nur zugewiesen werden soll, wenn eine Kennung mit dem angegebenen Wert gefunden wurde. Die Kennungsanforderung ist nur erfolgreich, wenn die hier ausgewählte Gruppe von Kriterien genau mit einer Kriteriengruppe übereinstimmt, die für mindestens einen Kennungspool in Terminal ID Management festgelegt wurde.

Kriterien für Terminal ID Management

Kriterium	Beschreibung
Poolname	Definieren Sie dieses Attribut, und geben Sie den Namen des Pools ein, um die Kennungssuche auf einen Pool einzugrenzen.
Client-IP-Adresse	Die IP-Adresse des Clientrechners wird in die Anforderung einer Kennung mit einbezogen.
Hostadresse	Die Adresse des für die Sitzung konfigurierten Hosts wird in die Anforderung einer Kennung mit einbezogen.
Hostport	Der Port des für die Sitzung konfigurierten Hosts wird in die Anforderung einer Kennung mit einbezogen.
Name der Sitzung	Wenn Sie diese Option wählen, muss die Kennung für die exklusive Verwendung durch die Sitzung konfiguriert sein.
Sitzungstyp	Der Sitzungstyp (z. B. IBM 3270, IBM 5250, UTS, ALC oder T27) ist immer in Anforderungen für eine Kennung enthalten.
Benutzername	Mit diesem Kriterium können Sie gewährleisten, dass ausschließlich zur exklusiven Verwendung durch bestimmte Benutzer erstellte Kennungen zugewiesen werden. Der Name des aktuellen Benutzers entspricht dem Benutzer, dem die Sitzung zur Laufzeit zugewiesen ist. Der Name muss in einer Kennung gefunden werden, um zugewiesen werden zu können. Für die Konfiguration einer auf Benutzernamen basierenden Sitzung ist ein Standardplatzhalter-Benutzername verfügbar: tidm-setup. Wenn ein Administrator Sitzungen mithilfe von tidm-setup konfigurieren möchte, muss Terminal ID Manager Kennungen für tidm-setup bereitgestellt haben. Sie können den Standardnamen mit einem eigenen Namen überschreiben, indem Sie die Datei `&ltInstallationsverzeichnis>/sessionserver/conf/container.properties` wie folgt ändern: `id.manager.user.name=benutzerdefinierter-Benutzername`. Dabei wird `benutzerdefinierter-Benutzername` durch den Namen ersetzt, den Sie verwenden möchten.
Anwendungsname (UTS)	Der Name der Hostanwendung wird in die Anforderung einer Kennung mit einbezogen.

Um das Verhalten bei der Verbindungsherstellung festzulegen, wenn Terminal ID Management für die betreffende Sitzung keine Kennung zuordnen kann, verwenden Sie **Bei nicht zugeordneter Kennung**:

- **Verbindungsversuch fehlschlagen lassen** – Wenn diese Option aktiviert ist, versucht die Sitzung nicht, eine Verbindung herzustellen, wenn eine Kennung nicht zugeordnet ist.
- **Verbindungsversuch zulassen** – Wenn diese Option aktiviert ist, versucht die Sitzung, eine Verbindung herzustellen, wenn eine Kennung nicht zugeordnet ist. Der Versuch kann jedoch vom Host abgelehnt werden. Bei einigen Hosttypen können Benutzer ohne Kennung eine Verbindung herstellen.

  Klicken Sie auf Terminal ID Manager-Kriterien testen, um zu bestätigen, dass Terminal ID Manager mithilfe der ausgewählten Kriterien und Werte eine Kennung bereitstellen kann.
- **Pakete zum Aktivhalten senden** – Verwenden Sie diese Einstellung, um die Verbindung zwischen Ihrer Sitzung und dem Host kontinuierlich zu überprüfen, sodass eventuelle Verbindungsprobleme zeitnah erkannt werden. Es stehen folgende Typen von Keep-Alive-Paketen zur Auswahl:

Option	Funktion
Keine	Standardeinstellung. Es werden keine Pakete gesendet.
System	Der TCP/IP-Stapel überwacht die Hostverbindung und sendet ab und zu Keep-Alive-Pakete. Bei dieser Option werden weniger Systemressourcen als bei den Optionen „NOP-Pakete senden“ oder „Taktmarkenpakete senden“ verwendet.
NOP-Pakete senden	Ein NOP-Befehl („No Operation“, keine Operation) wird in regelmäßigen Abständen an den Host gesendet. Der Host muss auf diese Befehle nicht antworten; der TCP/IP-Stapel kann jedoch feststellen, ob beim Zustellen des Pakets ein Problem auftritt.
Taktmarkenpakete senden	Ein Taktmarkenbefehl wird in regelmäßigen Abständen an den Host gesendet, um zu prüfen, ob die Verbindung noch aktiv ist. Der Host sollte auf diese Befehle antworten. Wenn keine Antwort eingeht oder beim Senden des Pakets ein Fehler auftritt, wird die Verbindung getrennt.

- **Zeitlimit zum Aktivhalten (Sekunden)** – Wenn Sie die Option „NOP-Pakete senden“ oder „Taktmarkenpakete senden“ auswählen, wählen Sie das Intervall zwischen den Sendeanforderungen zum Aktivhalten aus. Die Werte liegen zwischen 1 und 36000 Sekunden (eine Stunde); der Standardwert ist 600 Sekunden.

Terminal ID Manager-Kriterien testen

Terminal ID Management gibt zur Laufzeit Kennungen an Clientanwendungen aus. Verwenden Sie diese Testoption, um zu bestätigen, dass Terminal ID Management mithilfe der ausgewählten Kriterien und Werte eine Kennung bereitstellen kann.

Die Kriterien für die aktuelle Sitzung werden im Bereich „Verbindung“ angegeben, nachdem Sie entweder über den Gerätenamen (3270- und 5250-Hosttypen), das Feld „Terminalkennung (UTS)“ oder das Feld „Stationskennung“ (T27) die Option **Terminal ID Management verwenden** ausgewählt haben. Standardmäßig werden die ausgewählten Kriterien für die aktuelle Sitzung angezeigt.

Klicken Sie auf **Testen**, um zu überprüfen, ob Terminal ID Management eine Kennung bereitstellen kann, die mit den konfigurierten und ausgewählten Kriterien und Werten übereinstimmt. Der Test gibt den Namen einer verfügbaren Kennung zurück, die die ausgewählten Attributkriterien erfüllt.

Testen weiterer Kriterien und Werte

In diesem Bereich können Sie Kriterien testen, die sich von denen für die aktuelle Sitzung unterscheiden.

1. Wählen Sie beliebige Einträge aus der Liste „Sitzungstyp“ aus, und geben Sie die zu testenden Kriterien an. Sie können alternative Werte testen, die Sie in einer Terminal ID Management-Beispielanfrage verwenden möchten.
2. Klicken Sie auf **Testen**, um zu überprüfen, ob Terminal ID Management eine Kennung bereitstellen kann, die mit den ausgewählten Kriterien und Werten übereinstimmt. Der Test gibt den Namen einer verfügbaren Kennung zurück, die die ausgewählten Werte erfüllt.

4.3.3 3270- und 5250-Verbindungseinstellungen

3270- und 5250-Hosttypen erfordern neben den allgemeinen Verbindungseinstellungen die nachstehenden spezifischen Einstellungen.

- **Terminalmodell**

  Geben Sie das Terminalmodell (die Anzeigestation) an, das von Host Access for the Cloud emuliert werden soll. Je nach Hosttyp sind unterschiedliche Terminalmodelle verfügbar.

  Wenn Sie **Benutzerdefiniertes Modell** wählen, können Sie das Terminalmodell durch Festlegen der Anzahl der Spalten und Zeilen anpassen.

- **Automatische Kerberos-Anmeldung verwenden (nur 5250)** MSS

  Wenn dies auf **Ja** festgelegt ist, muss der Benutzer keine Anmeldeberechtigung eingeben. Die automatische Kerberos-Anmeldung wird unter „MSS-Verwaltungskonsole > Host Access for the Cloud“ konfiguriert. In Bezug auf die Konfiguration von HACloud zur Verwendung des Kerberos-Authentifizierungsprotokolls sollten Sie mit bestimmten Begriffen vertraut sein und die zu erfüllenden Voraussetzungen kennen, bevor Sie diese Option konfigurieren. Diese Optionen sind ausführlich in der Dokumentation im Bereich „Host Access for the Cloud“ der MSS-Verwaltungskonsole beschrieben, die über die Hilfe-Schaltfläche verfügbar ist. Weitere Informationen finden Sie unter Einrichten von Kerberos für Single Sign-on mit AS/400.

- **Terminalkennung** (nur 3270)

  Wenn Host Access for the Cloud eine Verbindung zu einem Telnet-Host herstellt, handeln das Telnet-Protokoll und der Host eine Terminalkennung aus, die während der anfänglichen Telnet-Verbindung verwendet wird. In der Regel einigen sich beide Seiten bei der Aushandlung auf die richtige Terminalkennung, sodass Sie dieses Feld leer lassen sollten.

- **TLS-Sicherheit**

  Über TLS-Protokolle können Clients und Server sichere, verschlüsselte Verbindungen in einem öffentlichen Netzwerk herstellen. Wenn Sie mithilfe von TLS Verbindungen herstellen, authentifiziert Host Access for the Cloud den Server, bevor eine Sitzung geöffnet wird. Alle Daten, die zwischen Host Access for the Cloud und dem Host übertragen werden, werden mit der ausgewählten Verschlüsselungsstufe verschlüsselt. Ausführliche Informationen zu dieser allgemeinen Einstellung finden Sie unter Allgemeine Verbindungseinstellungen.

- **Gerätename**

  Wenn Sie als Protokoll TN3270, TN3270E oder TN5250 ausgewählt haben, geben Sie den Gerätenamen an, der bei der Verbindung der Sitzung zum Host verwendet werden soll. Der

Gerätename ist auch unter der Bezeichnung Host-LU oder Pool bekannt. Zudem können Sie folgende Optionen auswählen:

- **Eindeutigen Gerätenamen generieren** – Generiert automatisch einen eindeutigen Gerätenamen.
- **Terminal ID Manager verwenden** – Zeigt zusätzliche Einstellungen zum Festlegen an. Siehe Verwenden von Terminal ID Manager.
- **Benutzer immer zur Eingabe der ID auffordern** – Der Endbenutzer wird bei jedem Verbindungsversuch aufgefordert, die Geräte-ID einzugeben.
- **Benutzer zur Eingabe auffordern, falls ID nicht angegeben** – Der Endbenutzer wird beim ersten Verbindungsversuch zur Eingabe aufgefordert und der eingegebene Wert wird gespeichert. Der gespeicherte Wert wird dann ohne weitere Aufforderungen verwendet.

Wenn Sie für die Sitzung keinen Gerätenamen angeben, weist der Host der Sitzung dynamisch einen Namen zu. Wenn ein Gerätename in einem Makro festgelegt ist, wird diese Einstellung überschrieben.

4.3.4 VT-Verbindungseinstellungen

VT-Hosts erfordern neben den allgemeinen Verbindungseinstellungen die folgenden zusätzlichen Einstellungen. Diese Einstellungen sind je nach dem verwendeten Protokoll (Telnet oder SSH) unterschiedlich. Die Einstellungen gelten für beide Protokolle, sofern nicht anders vermerkt.

Konfigurationsoptionen für VT-Sitzungen

VT-Einstellungen	Beschreibung
Terminalkennung	Diese Einstellung legt fest, welche Antwort Host Access for the Cloud nach einer primären Geräteattributanforderung an den Host sendet. Anhand der Antwort kann der Host erkennen, welche Terminalfunktionen ausgeführt werden können. Die für die jeweilige Terminalkennung von Host Access for the Cloud gesendete Antwort entspricht genau der Antwort des VT-Terminals; einige Anwendungen erfordern unter Umständen eine spezifische Geräteattributantwort. Diese Einstellung für die Terminalkennung ist unabhängig von der Option im Feld „Terminaltyp“. Die Optionen lauten: VT220, VT420, VT100, DEC-VT100 und VT52.
Unbekannte Hosts zulassen (SSH)	Mit dieser Einstellung kann der Administrator entscheiden, ob der Webclient alle unbekannten Hosts erkennen soll. Die folgenden Optionen stehen zur Auswahl: • **Ja**: Unbekannte Hosts und alle SSH-Verbindungen sind zulässig. Webclient-Benutzer werden nicht gefragt, ob den Hosts vertraut werden soll. • **Fragen**: Bei einer Verbindung zu einem noch unbekannten Host wird der Benutzer des Webclients gefragt, ob dem Host vertraut werden soll. Lautet die Antwort „Ja“, dann wird sein öffentlicher Schlüssel in den Benutzereinstellungen gespeichert. Bei darauffolgenden Verbindungen wird die obige Frage erst wieder gestellt, wenn sich der Schlüssel des Hosts ändert. • **Nein**: Unbekannte Hosts werden nie zugelassen. Nur Hosts, die der Administrator beim Konfigurieren der Sitzung als vertrauenswürdig einstuft, werden zugelassen. Endbenutzer werden nie gefragt und die Sitzung endet je nach der Auswahl des Administrators in einer Verbindung oder nicht.
Bannermeldungen unterdrücken (SSH)	Wenn diese Option aktiviert ist, wird der SSH-Banner nicht angezeigt. Diese Option ist bei der Aufzeichnung von Makros für die SSH-Anmeldung hilfreich.
Lokales Echo (Telnet)	Automatisch (Standard). Hier wird festgelegt, wie Host Access for the Cloud auf das Echo eines Telnet-Hosts antworten soll: Wenn die Option auf „Automatisch“ festgelegt ist, wird versucht, mit dem Host ein Remoteecho auszuhandeln, es werden jedoch die Befehle des Hosts ausgeführt. Wenn die Option auf „Ja“ festgelegt ist, handelt Host Access for the Cloud ein lokales Echo mit dem Host aus, wobei jedoch immer ein Echo ausgeführt wird, während Host

	Access for the Cloud bei der Option „Nein“ ein Remoteecho mit dem Host aushandelt, aber kein Echo ausführt.
Echo neu vereinbaren (Telnet)	Nein (Standard). Wenn diese Option auf „Ja“ festgelegt ist, werden Passwörter auf dem lokalen Bildschirm nicht angezeigt. Alle anderen Arten von eingegebenem Text sind hingegen sichtbar. Host Access for the Cloud unterstützt die Telnet-Option „Suppress Local Echo“ (SLE, Lokales Echo unterdrücken), wenn die Verbindung mit einem Host im Halbduplexmodus hergestellt wird. Das bedeutet, dass Host Access for the Cloud das Zeichenecho zum Hostcomputer unterdrückt. Mit SLE-Unterstützung kann Host Access for the Cloud angewiesen werden, das Echo lokal zu unterdrücken.
Hostfenstergröße festlegen	Ja (Standard). Wenn dieses Kontrollkästchen aktiviert ist, wird die Anzahl der Spalten und Zeilen bei jeder Änderung an den Host gesendet. Dadurch kann der Telnet-Host auch bei einer Änderung der Fenstergröße den Cursor richtig steuern.
Binär-Modus (Telnet)	Nein (Standard). Telnet gibt einen 7-Bit-Datenpfad zwischen dem Host und dem Terminal vor. Diese Art von Datenpfad ist mit bestimmten nationalen Zeichensätzen nicht kompatibel. Allerdings lassen viele Hosts auch 8-Bit-Zeichen zu, ohne dass dabei das achte Bit den Wert null annehmen muss. In bestimmten Fällen muss der Host jedoch explizit angewiesen werden, im 8-Bit-Modus zu arbeiten. Dies geschieht durch das Aktivieren dieses Kontrollkästchens.
LF nach CR senden (Telnet)	Nein (Standard). Ein „echter“ Telnet-Host erwartet, dass eine vom Terminal gesendete Zeile durch die Steuerzeichenfolge „CrNu“ (Wagenrücklauf/Null) abgeschlossen wird. Bei einigen im Internet verfügbaren Hosts handelt es sich jedoch nicht um echte Telnet-Hosts. Diese Hosts erwarten zur Kennzeichnung von Zeilenenden nach dem CR-Zeichen ein Lf-Zeichen (Line Feed = Zeilenvorschubzeichen). Wenn Sie eine Verbindung zu einem solchen Host herstellen möchten, wählen Sie „Ja“.
Strg+Untbr sendet (Telnet)	Wählen Sie aus, welche Sequenz beim Drücken von Strg+Untbr an den Host gesendet wird. Optionen sind: „Telnet-Abbruch“ (Standard), „Prozess unterbrechen“ oder „Nichts“.
Hostzeichensatz	Der Standardwert für den Hostzeichensatz hängt von dem jeweils emulierten Terminaltyp ab. Diese Einstellung zeigt den aktuellen Terminalstatus des VT-Hostzeichensatzes an, der durch den Host

	geändert werden kann. Die entsprechende, in dem Modell gespeicherte Standardeinstellung lautet „DEC Supplemental“.
Automatische Antwort	Nein (Standard). Diese Einstellung gibt an, ob der Antworttext (der über die Eigenschaft „Answerback“ eingerichtet wird) nach dem Aufbau einer Verbindung automatisch an den Host gesendet werden soll.
Antworttext	Mithilfe dieser Einstellung können Sie im Textfeld einen Antworttext eingeben, wenn der Host eine Antwort auf ein ENQ-Zeichen erwartet. Der Antworttext unterstützt Zeichen mit Codes kleiner oder gleich 0xFFFF als Unicode-Escape-Sequenzen. Die Escape-Sequenz beginnt mit \u gefolgt von genau vier Hexadezimalziffern. Unicode-Escape-Sequenzen können in beliebige Zeichenketten eingebettet werden. So wird beispielsweise dieses eingebettete \u0045 als dieses eingebettete E interpretiert, da 45 der Hexadezimalcode für den Buchstaben E ist. Für die Übergabe der Unicode-Escape-Sequenzen an den Host stellen Sie der Sequenz einen Backslash voran. Soll beispielsweise der Buchstabe \u001C an den Host gesendet werden, belegen Sie eine Taste mit \\u001C. Beim Drücken dieser Taste wandelt Host Access for the Cloud dies in die Zeichenkette \u001C um und sendet die 6 Zeichen der daraus entstehenden Zeichenkette an den Host.

Weitere Informationen

- TLS-Beschreibungen

4.3.5 UTS-Verbindungseinstellungen

UTS-Hosts erfordern neben den allgemeinen Verbindungseinstellungen die folgenden zusätzlichen Einstellungen:

Konfigurationsoptionen für UTS INT1-Sitzungen

UTS INT1-Optionen	Beschreibung
Anwendung	Der Name der Hostanwendung oder des Hostbetriebsmodus, auf die bzw. den zugegriffen wird. Dieses Wort bzw. diese Wortgruppe wird bei der ersten Verbindungsherstellung zum Host vom lokalen Computer an den Host gesendet. Wenn Sie ein Hostterminal verwenden, wäre dies der $$OPEN-Name der Anwendung. Der Name der Anwendung entspricht in der Regel dem Namen der Umgebung. Die Namen können allerdings auch voneinander abweichen. Ein Beispiel: Der Name der Umgebung lautet MAPPER, und der Name der Anwendung lautet UDSSRC. Während einer Terminalemulationssitzung geben Sie in der Eingabeaufforderung $$OPEN MAPPER ein. Wenn die Verbindung hergestellt wurde, sendet INT1 den Namen UDSSRC an den Host.
TSAP	Der gewünschte Transport Service Access Point (TSAP), bis zu 32 Zeichen (z. B. TIPCSU für TIP-Verbindungen, RSDCSU für Demand-Verbindungen). Ein TSAP ist nur dann erforderlich, wenn Sie im IP-Router-Modus eine Verbindung zu einem Host-LAN-Controller (HLC) oder verteilten Kommunikationsprozessor (DCP, Distributed Communications Processor) herstellen. Wenn Sie nicht sicher sind, welchen Wert Sie verwenden müssen, wenden Sie sich an Ihren Hostadministrator.
Ausgangstransaktion	Das Zeichen oder das Wort bzw. die Wortgruppe, das bzw. die der lokale Computer an den Host sendet, wenn zum ersten Mal eine Verbindung mit dem Host hergestellt wird (bis zu 15 Zeichen). Dieser optionale Parameter wird in der Regel mit TIP verwendet. Sie können beispielsweise ^ eingeben, um MAPPER auszuführen. Dieser Parameter kann außerdem für die Übertragung von Passwörtern verwendet werden.
Transaktion starten	Wenn Sie eine Ausgangstransaktion konfigurieren, werden die Daten standardmäßig gesendet, sobald die Verbindung zur Sitzung hergestellt wurde. Sie können selbst entscheiden, wann eine Ausgangstransaktion gesendet wird, indem Sie die Ausgangstransaktion mithilfe einer bestimmten Zeichenfolge auslösen. Wenn Sie beispielsweise erst dann die Daten der Ausgangstransaktion senden möchten, wenn die Anmeldung erfolgreich war, geben Sie eine Zeichenkette ein, die zum Identifizieren einer erfolgreichen Anmeldung verwendet wird.

	Sie können diese Einstellung zusammen mit **Ausgangstransaktion senden** verwenden.
Ausgangstransaktion senden	Sie können festlegen, wann die Ausgangstransaktion gesendet werden soll: • **Sofort** (Standard). • **Wenn das Zeichen für den Anfang des Eintrags empfangen wird** – Diese Einstellung ist hilfreich, wenn mehrzeilige Transaktionen abgeschlossen sein müssen, bevor die Zeichenfolge gesendet wird. • **Nach angegebenen Millisekunden**
Terminalkennung	Wählen Sie die gewünschten Optionen zum Festlegen einer Terminalkennung oder zum Verwenden von Terminal ID Manager aus. Um eine Terminalkennung festzulegen, geben Sie sie im Feld **Terminalkennung angeben** ein. • Terminalkennung angeben Die Terminalkennung (in der Regel bis zu acht alphanumerische Zeichen), die für die mit diesem Pfad verknüpfte Kommunikationssitzung verwendet werden soll. Jede Terminalkennung (auch TID oder PID genannt) muss für den jeweiligen Host eindeutig sein. • Benutzer zur Eingabe auffordern, falls ID nicht angegeben : Der Endbenutzer wird beim ersten Verbindungsversuch zur Eingabe aufgefordert und der eingegebene Wert wird gespeichert. Der gespeicherte Wert wird dann ohne weitere Aufforderungen verwendet. • Benutzer immer zur Eingabe der ID auffordern : Wenn Sie diese Option auswählen, wird der Endbenutzer bei jedem Verbindungsversuch zur Eingabe der Terminalkennung aufgefordert. • Terminal ID Manager verwenden Wenn Sie **Terminal ID Manager verwenden** auswählen, werden Sie aufgefordert, die Attribute der Terminalkennung auszuwählen, die Sie für den Abruf einer Kennung verwenden möchten. Weitere Informationen finden Sie unter „Terminal ID Manager-Attribute“. Klicken Sie auf **Testen**, um die Attribute zu prüfen.

Weitere Informationen

- Terminal ID Manager-Attribute
- TLS-Beschreibungen

4.3.6 T27-Verbindungseinstellungen

Neben den allgemeinen Verbindungseinstellungen können Sie die folgenden zusätzlichen T27-Verbindungsoptionen konfigurieren:

T27-Verbindungseinstellungen

T27-Optionen	Beschreibung
Terminaltyp	Wählen Sie den Terminaltyp aus, der während der Sitzung emuliert wird. Bei der T27-Emulation werden Unisys TD830, TD830 ASCII, TD830 INTL und TD830 NDL als Terminaltypen unterstützt..
Binär-Modus	Sie müssen die Option „Binär-Modus“ aktivieren, wenn Passthrough-Drucken erforderlich ist. Der Standardwert ist "Nein". TCPA gibt einen 7-Bit-Datenpfad zwischen dem Host und dem Terminal vor. Diese Art von Datenpfad ist mit bestimmten nationalen Zeichensätzen nicht kompatibel. Allerdings lassen viele Hosts auch 8-Bit-Zeichen zu, ohne dass dabei das achte Bit den Wert Null annehmen muss. Es kann jedoch erforderlich sein, den Host zur Verwendung eines 8-Bit-Datenpfads zu zwingen. Dazu können Sie diese Option auswählen.
Zeilenbreite	Wählen Sie die Anzahl der Zeichen aus, die der Host an den Client sendet. Die Standardeinstellung sind 80 Zeichen.
TLS-Sicherheit	Eine Beschreibung der verschiedenen Optionen finden Sie unter **TLS-Beschreibungen**.
Stationskennung	Wählen Sie aus, ob Sie selbst eine Stationskennung angeben oder dazu Terminal ID Manager verwenden möchten. Wählen Sie zum Angeben einer Stationskennung die Option **Stationskennung angeben** und geben Sie den Namen im Feld „Stationskennung“ ein. Jede Stationskennung muss für den Host eindeutig sein und besteht normalerweise aus bis zu acht alphanumerischen Zeichen. • Benutzer zur Eingabe auffordern, falls ID nicht angegeben : Der Endbenutzer wird beim ersten Verbindungsversuch zur Eingabe aufgefordert und der eingegebene Wert wird gespeichert. Der gespeicherte Wert wird dann ohne weitere Aufforderungen verwendet. • Benutzer immer zur Eingabe der ID auffordern : Wenn Sie diese Option auswählen, wird der Endbenutzer bei jedem Verbindungsversuch zur Eingabe der Stationskennung aufgefordert. • Terminal ID Manager verwenden Wenn Sie „Terminal ID Manager verwenden“ auswählen, werden verschiedene zu konfigurierende Kriterien für die Terminalkennung angezeigt. Eine Beschreibung der verschiedenen Optionen finden Sie unter **Kriterien für Terminal ID Manager**.

Wenn Sie für die Sitzung keine Stationskennung angeben, weist der Host der Sitzung dynamisch eine Kennung zu.

Weitere Informationen

- TLS-Beschreibungen
- Kriterien für Terminal ID Manager

4.3.7 ALC-Verbindungseinstellungen

ALC-Hosts erfordern neben den allgemeinen Verbindungseinstellungen die folgenden zusätzlichen Einstellungen:

ALC-Verbindungseinstellungen

ALC-Optionen	Beschreibungen
TLS-Sicherheit	Eine Beschreibung der verschiedenen Optionen finden Sie unter **TLS-Beschreibungen**.
Zeichencodierung	Wählen Sie ASCII, EBCDIC oder IPARS (Standard) als Codesatz aus.
Konfigurationsdatei	Geben Sie die Konfigurationsdatei (CNF-Datei) ein, mit der Konfigurationsinformationen für einen spezifischen Hosttyp zugeordnet werden.
Terminaladresse	Wählen Sie aus, ob Sie die Terminaladresse angeben oder Terminal ID Management verwenden möchten. • **Terminaladresse** – Geben Sie an, ob der 2-Byte- oder der 4-Byte-Adressierungsmodus verwendet werden soll. Obwohl eine eindeutige 5-Byte-Adresse erforderlich ist, wenn Sie die Terminalkennung angeben anstatt ID Manager zu verwenden, wird über diese Option angegeben, wie viele Bytes der 5-Byte-Terminaladresse mit jeder Nachricht zum Zweck des Multiplexing gesendet werden. Wenn Sie den 2-Byte-Adressierungsmodus angeben, werden nur die letzten 2 Byte der ASCU (Agent Set Control Unit)-Clusteradresse (A1, A2) gesendet. Wenn Sie den 4-Byte-Adressierungsmodus angeben, wird die vollständige ASCU-Clusteradresse (H1, H2, A1, A2) gesendet. Geben Sie die eindeutige 5-Byte-Terminaladresse für diese Sitzung an. Die Terminaladresse besteht aus fünf 2-stelligen hexadezimalen Werten in folgender Reihenfolge: H1, H2, A1, A2 und TA (Terminaladresse). Diese eindeutige Adresse wird im Allgemeinen vom Netzwerkadministrator zugewiesen. • **Terminal ID Management**: Gibt zur Laufzeit Kennungen an Clientanwendungen aus. Wenn Sie diese Option auswählen, müssen zusätzliche Konfigurationsoptionen festgelegt werden. Eine Beschreibung dieser Optionen finden Sie unter **Kriterien für Terminal ID Management**.

Weitere Informationen

- TLS-Beschreibungen
- Kriterien für Terminal ID Manager

4.4 Bereitstellen von Zugriff auf Hostsitzungen

Die Endbenutzer greifen entweder über einen Sitzungsserver oder über die Liste „Assigned Sessions“ (Zugewiesene Sitzungen) auf Sitzungen zu. Bei beiden Optionen wird den Benutzern nach der Authentifizierung eine Liste der Sitzungen angezeigt, auf die sie zugreifen und die sie starten können.

> **Tipp**
>
> Die Verwendung eines Lastverteilers zur Gewährleistung der Hochverfügbarkeit und Skalierbarkeit wird dringend empfohlen. Weitere Informationen finden Sie unter Planen der Bereitstellung.

4.4.1 Sitzungsserver

Üblicherweise greifen die Benutzer über die Sitzungsserver, typischerweise über einen Lastverteiler, auf die Sitzungen zu.

Der Endbenutzerzugriff auf dem Sitzungsserver erfolgt über `https://<Sitzungsserver>:7443/`.

4.4.2 Liste „Assigned Sessions“ (Zugewiesene Sitzungen)

Mithilfe der Liste „Assigned Sessions“ (Zugewiesene Sitzungen) können die Benutzer von einem konsolidierten, HTML-basierten Portal auf alle ihre Sitzungen zugreifen. Nach der Authentifizierung wird dem Benutzer die Liste der zugewiesenen Sitzungen angezeigt.

Die Liste „Assigned Sessions“ (Zugewiesene Sitzungen) ist unter `https://<MSS-Server>/sessions/` verfügbar.

Informationen zum Konfigurieren der Liste „Assigned Sessions“ (Zugewiesene Sitzungen) finden Sie unter Konfigurieren der Liste „Assigned Sessions“ (Zugewiesene Sitzungen).

4.5 Verwalten der Benutzereinstellungen

Als Administrator können Sie auswählen, welche Optionen Benutzer für ihre Sitzungen konfigurieren dürfen. Die Optionen werden für die jeweilige Sitzung festgelegt. So können alle Benutzer, die Zugriff auf eine bestimmte Sitzung haben, ihre eigene Sitzungsinstanz konfigurieren.

1. Wählen Sie im linken Navigationsbereich die Option **Regeln für Benutzereinstellungen** aus.
2. Wählen Sie aus, welche Optionen die Benutzer konfigurieren können.
3. Klicken Sie auf Speichern.

Die einzelnen Konfigurationen gelten speziell für die Instanz der jeweiligen Sitzung und stehen nicht in Konflikt mit den Einstellungen der anderen Benutzer.

In den verschiedenen Einstellungs- und Anzeigebereichen ist eine Option **Standardeinstellungen wiederherstellen** verfügbar. Wenn von einem Administrator ausgeführt, stellt diese Option den Webclient auf die standardmäßigen Einstellungen zurück. Für Endbenutzer stellt diese Option die vom Administrator beim Erstellen der Sitzung festgelegten Werte wieder her.

> **Achtung**
>
> Beachten Sie, dass alle Benutzer die gleichen Einstellungen teilen, wenn die Authentifizierungsmethode auf „Keine“ festgelegt ist. In diesem Fall empfiehlt es sich, in der Sitzungskonfiguration den Benutzern das Ändern der Sitzungseinstellungen zu verbieten (Regeln für Benutzereinstellungen), um zu verhindern, dass die Benutzer sich gegenseitig die Einstellungen überschreiben. Um dieses Problem zu umgehen, besteht die Möglichkeit, Benutzeridentitäten auf andere Weisen bereitzustellen.

Weitere Informationen

- Anzeigeeinstellungen
- Angeben von Bearbeitungsoptionen
- Dateiübertragung
- Erstellen von Makros

4.6 Anpassen von Hostsitzungen

4.6.1 Anpassen von Hostsitzungen

Zur Anpassung von Sitzungen von Endbenutzern stehen folgende Funktionen zur Verfügung:

- **Plus** – Aktiviert benutzerdefinierte Steuerelemente, um effizientere Abläufe und eine moderne und benutzerfreundliche Oberfläche zu bieten. Siehe „Anpassen von Bildschirmen mithilfe von ‚Plus'".

  Mit dieser Option können Sie QuickInfos in Felder einfügen und nummerierte Listen durch modernere Dropdownlisten ersetzen. Weiterhin können Sie Schaltflächen zur Hostoberfläche hinzufügen und zum Starten von Makros oder zum Durchführen anderer Aktionen programmieren und die manuelle Datumseingabe durch einen Kalender ersetzen, aus dem Daten ausgewählt werden können.

- **Serverseitige Ereignisse** – Stellt prozedualen Java-Code bereit, mit dem die Darstellung von Hostdaten erweitert und verbessert wird.

  Mit serverseitigen Ereignissen können sie spezifische Ereignisse definieren und die Hostanwendung anhalten, ersetzen oder mit für die Sitzung bereitgestelltem Code unterbrechen. Außerdem können Sie die Optionen für die Fehlerbehandlung erweitern. Beispielsweise können Sie ein Ereignis hinzufügen, das Fehler erkennt und Code implementiert, um den Fehler abzufangen, zu kontrollieren und zu beheben. Siehe Serverseitige Ereignisse.

- **Erweitert** – Verwenden Sie diese Option nur nach Anweisung durch den technischen Support von Micro Focus.

Diese Optionen werden im Bereich „Anpassung" konfiguriert.

1. Klicken Sie in der Symbolleiste auf Einstellungen, um den linken Navigationsbereich zu öffnen.
2. Klicken Sie auf Anpassung.

Weitere Informationen

- Anpassen von Bildschirmen mithilfe von „Plus"
- Verwenden serverseitiger Ereignisse

4.6.2 Anpassen von Bildschirmen mithilfe von „Plus“

> **Hinweis**
>
> Für die Funktion „Plus“ sind Archivdateien (`.rdar`) erforderlich, die mit Micro Focus Screen Designer Version 9.5 oder höher generiert wurden. Der Bildschirmeditor ist in Micro Focus Rumba Desktop 9.5 verfügbar. Reflection Desktop 16.1 umfasst eine eingeschränkte Version des Bildschirmeditors. Um auf weitere Steuerelemente zugreifen und alle Funktionen von Plus und des Bildschirmeditors nutzen zu können, können Sie das Micro Focus Reflection Desktop Plus-Add-On erwerben und installieren.

1. Klicken Sie im Bereich **Anpassung** auf **Plus aktivieren**.
2. Wählen Sie in der Dropdown-Liste die gewünschte Plus-Archivdatei aus oder laden Sie eine Datei aus einem anderen Speicherort hoch. Plus-Archivdateien sind an der Dateinamenerweiterung `rdar` erkennbar.

   Archivdateien sind die Ausgabe eines Screen Designer-Projekts und werden zum Bereitstellen der benutzerdefinierten Steuerkriterien verwendet.

   Wenn Sie die Plus-Archivdatei (`.rdar`) aktualisieren, die der Sitzung mit Plus-Aktivierung zugeordnet ist, müssen Sie zunächst den Ordner mit der alten RDAR-Datei auf dem Sitzungsserver löschen. Nach dem Löschen des Ordners können Sie die Sitzung mit Plus-Aktivierung öffnen und die neue RDAR-Datei wird auf den Sitzungsserver heruntergeladen.
3. Überprüfen Sie, ob die Einstellung der Anzahl an Millisekunden für die Hostaufbauverzögerung korrekt ist. Dies ist die Zeit, die der Server auf die Herstellung einer synchronen Verbindung wartet, bevor er davon ausgeht, dass der Host die Datenübertragung abgeschlossen hat.
4. Wenn Sie zu der Sitzung zurückkehren, ist Plus verfügbar. Klicken Sie auf der Symbolleiste auf  , um die benutzerdefinierten Steuerelemente zu deaktivieren.

Wenn Sie Plus für eine Sitzung aktivieren, sehen alle Endbenutzer dieser Sitzung auf der Symbolleiste das Plus-Symbol und alle Steuerelemente, die über die Transformationsdatei des Bildschirmeditors zur Verfügung gestellt werden.

Weitere Informationen

- Anpassen von Hostsitzungen

4.6.3 Verwenden serverseitiger Ereignisse

Über serverseitige Ereignisse können Sie prozeduralen Java-Code bereitstellen, mit dem die Darstellung von Hostdaten erweitert und verbessert wird.

Im Bereich „Anpassung“ wird für den Webclient angegeben, wo das Ereignis gefunden werden kann, nachdem Sie dies konfiguriert haben. Anweisungen zur Verwendung des SDK und den verfügbaren Beispielen finden Sie unter Verwenden des Java-SDK.

1. Öffnen Sie den Bereich **Anpassung**.
2. Geben Sie unter **Serverseitige Ereignisse** den vollständigen Klassennamen für das Ereignis ein.
3. Starten Sie die Sitzung und testen Sie das Ereignis.

Greifen Sie auf die API-Dokumentation und Ereignisbeispiele zu.

Weitere Informationen

- Anpassen von Hostsitzungen
- Verwenden des Java-SDK
- Entwicklung

4.7 Protokollierung

4.7.1 Speicherort der Protokolldateien

Zwei Protokolldateien stehen zur Verfügung:

- `<Installationsverzeichnis>/sessionserver/sessionserver.log` : Protokolldatei für die Sitzungsserveranwendung.
- `<Installationsverzeichnis>/sessionserver/container.log` : Protokolldatei für den Container, der als Host für die Host Access for the Cloud-Anwendung dient.

4.7.2 Konfigurieren der Protokollrotation

Sie können die Protokollrotation durch Bearbeiten der Werte in `<Installationsverzeichnis>\sessionserver\microservices\sessionserver\service.yml` konfigurieren:

```
LOGGING_FILE_MAXSIZE
LOGGING_FILE_MAXHISTORY
```

4.7.3 Festlegen von Protokollierungsstufen

Es gibt verschiedene Typen von Protokollierungsstufen, mit denen unterschiedliche Arten von Informationen generiert werden können. Sie können den Protokollierumfang in `<Installationsverzeichnis>\sessionserver\microservices\sessionserver\service.yml` konfigurieren.

> **Hinweis**
>
> Zeilen in `service.yml` müssen mit Leerzeichen eingerückt werden.

Verwenden Sie zum Festlegen von Protokollierungsstufen das folgende Format:

```
- name: logging.level.<Protokollierung>
  value: "<Protokollierungsstufe>"
```

Dabei steht `<Protokollierung>` für den Namen der anzupassenden Protokollierung, und `<Protokollierungsstufe>` gibt eine der folgenden Stufen an:

- **Trace** – Gibt detailliertere informative Ereignisse an als „Debug“.
- **Debug** – Gibt informative Ereignisse auf Detailebene an, die sich besonders für die Fehlersuche bei einer Anwendung eignen.
- **Info** – Gibt Informationsmeldungen an, die den Fortschritt der Anwendung auf allgemeiner Ebene hervorheben.
- **Warn** – Gibt potenziell gefährliche Situationen an.
- **Error** – Gibt Fehlerereignisse an, bei denen die Anwendung trotzdem weiterhin ausgeführt werden könnte.
- **Fatal** – Gibt sehr schwerwiegende Fehlerereignisse an, die sehr wahrscheinlich zu einer Beendigung der Anwendung führen.

> **Hinweis**
>
> Nachdem Sie Änderungen an `service.yml` vorgenommen haben, müssen Sie den Sitzungsserver neu starten.

4.7.4 Aktivieren der Protokollierung vom Webclient zum Sitzungsserver

Der Browser bietet einen einfachen Mechanismus zur Protokollierung in seiner JavaScript-Konsole. Der Webclient erweitert diese Fähigkeit, sodass Sie mit einer entsprechenden Konfiguration Ereignisse auf dem Sitzungsserver protokollieren können, wo sie der Administrator anzeigen kann.

Standardmäßig erfolgt keine Protokollierung auf dem Sitzungsserver. Zum Aktivieren dieser Funktion müssen Sie den **Protokollierumfang festlegen**, indem Sie die unten aufgeführten Anweisungen befolgen.

Die verfügbaren Einstellungen für den Protokollumfang sind: `debug` (Fehlersuche), `info` (Information), `warn` (Warnung), `error` (Fehler) und `off` (keine Protokollierung). Standardmäßige ist der Protokollierumfang auf `off` eingestellt, d. h. deaktiviert.

Protokollierumfang für alle Webclient-Benutzer anpassen

Um den Protokollierumfang für alle Webclients anzupassen, fügen Sie den folgenden Eintrag zur Datei `<Installationsverzeichnis>\sessionserver\microservices\sessionserver\service.yml` hinzu:

```
-name: <Protokollierer>
 value: "<Protokollierumfang>"
```

`<Protokollier>` ist:

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

> **Hinweis**
>
> Gehen Sie mit Bedacht vor, wenn Sie den Protokollierumfang für alle Webclient-Benutzer in einer Produktionsumgebung erhöhen, weil dies den Netzwerkverkehr erhöhen kann.

Protokollierumfang für einen einzelnen Benutzer anpassen

Es gibt zwei Optionen zum Anpassen des Protokollierumfangs für einzelne Benutzer:

- Um vorübergehend den Protokollierumfang für die Webclient-Instanz eines bestimmten Benutzers anzupassen, ohne den Sitzungsserver neu zu starten, weisen Sie den Benutzer an, beim Laden des Webclients im Browser den folgenden URL-Parameter hinzuzufügen:

  `-https://meinssitzungsserver.com:7443/?log=<Protokollierumfang>-`

- Um den Protokollierumfang für einen einzelnen Benutzer anzupassen, ohne dass der Benutzer dazu Änderungen vornehmen muss, fügen Sie den folgenden Eintrag zur Datei `service.yml` hinzu:

  ```
    -name: <Protokollierer>
     value: "<Protokollierumfang>"
  ```

  `<Protokollier>` ist:

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

  `<Benutzername>` ist der Benutzername der Person, für die Sie den Protokollierumfang anpassen möchten.

> **Hinweis**
>
> Zur Protokollierung auf Basis eines Benutzernamens ist ein Authentifizierungsmodus erforderlich, der Benutzernamen verwendet.

5. Arbeiten mit HACloud

5.1 Verwenden von Host Access for the Cloud

Es stehen verschiedene Sitzungs- und Anzeigeoptionen zur Verfügung, damit Sie Ihre Sitzung personalisieren und eine effiziente Arbeitsweise sicherstellen können.

- Anzeigeeinstellungen
- Zuordnung von Tasten
- Konfigurieren von Benutzermakros
- Dateiübertragung
- Angeben von Bearbeitungsoptionen
- Verwenden von Sitzungen
- Erstellen von Makros
- Druckvorgang

5.2 Anzeigeeinstellungen

Die Anzeigeeinstellungen sind je nach Hosttyp unterschiedlich und jeweils für die konfigurierte Sitzung spezifisch.

5.2.1 Farbzuordnung

Sie können die Farbe Ihres Bildschirms und das Aussehen der verschiedenen Hostattribute im Terminalfenster anpassen. Sie können für jedes Element die Vorder- und Hintergrundfarben für alle unterstützten Hostverbindungen auswählen. Farben werden mithilfe der Farbpalette oder durch Eingabe des Hex-Code-Formats angegeben.

Die verfügbaren Hex-Farben werden auf zahlreichen Websites angeboten. Ein Beispiel dazu finden Sie unter w3schools.com HTML Color Picker.

Abhängig vom Typ der Hostverbindung sehen Sie möglicherweise unterschiedliche Optionen.

Spezifische Optionen für UTS-Hosts

- **Farbinformationen vom Host verwenden** –Deaktivieren Sie diese Option, um anstelle der durch den Host angegebenen Farben die hier angegebenen Farben zu verwenden.
- **Blinken Ein** – Wenn Sie das Blinken ausschalten möchten, deaktivieren Sie diese Option.
- **Attribut zur Bearbeitung auswählen** – In UTS-Emulationen werden Farben direkt vom Host eingestellt. Sie können für Text mit spezifischen Bildschirmanzeigeoptionen unterschiedliche Farben angeben. Dazu sind die folgenden Kombinationen verfügbar:

  Einfach, Unterstrichen (UND), Durchgestrichen (STK), Linkes Spaltentrennzeichen (LCS), Steuerungsseite und Statuszeile (OIA).
- **Videointensität** - Die Videointensitäten Blinken, Schwach, Geschützt und Invertiert werden für die Erstellung zusätzlicher Kombinationen mit den Attributen kombiniert. Sie können beispielsweise alle Vordergrund- und Hintergrundfarben mit Schwach + Blinken + Unterstrichen oder Invertiert + Geschützt + Durchgestrichen + Unterstrichen verknüpfen.

Wenn Sie eine Videointensität (oder eine Kombination verschiedener Intensitäten) auswählen, werden diese Intensitäten mit dem Wert aus der Dropdownliste „Attribut“ kombiniert und bilden so eine einzelne Farbzuordnung.

Spezifische Optionen für VT- und T27-Hosts

- **Blinken Ein** – Wenn Sie das Blinken ausschalten möchten, deaktivieren Sie diese Option.
- **Fettschrift Ein** – Zeigt Textabschnitte mit Fettattributen im Terminalfenster als fett formatierten Text an. Wenn fett formatierte Zeichen als Normaltext angezeigt werden sollen, deaktivieren Sie diese Option.

- **Unterstreichen ein** – Zeigt Text mit Unterstrich an.
- **Invertierte Darstellung (nur VT)** – Mit dieser Option werden die Vordergrund- und Hintergrundfarben umgekehrt, wenn der VT-Host eine invertierte Video-Escape-Sequenz sendet. Wenn diese Option deaktiviert ist, werden die vom Host gesendeten invertierten Videosequenzen ignoriert.

So passen Sie für alle Hosttypen die Farben an

1. Klicken Sie im linken Navigationsbereich auf „Anzeige“.
2. Klicken Sie unter „Farbzuordnungen“ auf das Hintergrundfarbenfeld, um die Farbpalette zu öffnen. Wählen Sie aus der Farbpalette die gewünschte Hintergrundfarbe für den Host aus. Alternativ dazu geben Sie die Nummer der gewünschten Hex-Farbe ein.
3. Wählen Sie aus der Dropdownliste die Standard-Hostfarbe aus, die Sie ändern möchten. Wenn Sie zum Beispiel „Host Rosa“ aus der Dropdown-Liste auswählen und dann die Vordergrundfarbe in Rot ändern, wird rosa Text immer rot dargestellt.
4. Öffnen Sie die Farbpalette für den Vordergrund, um eine Farbe auszuwählen, die dem Text zugewiesen werden soll. Alternativ können Sie manuell den gewünschten Hex-Code eingeben. Wählen Sie „Hintergrund“ aus, um die neue Farbe dem Feld „Hintergrund“ zuzuweisen.
5. Klicken Sie auf „Speichern“, um den Anzeigebereich zu schließen und mit der Konfiguration der Hostverbindung fortzufahren.

Über „Standardeinstellungen wiederherstellen“ löschen Sie alle vorgenommenen Änderungen und setzen die Werte für die Farben auf die standardmäßigen Hosteinstellungen zurück.

5.2.2 Konfigurieren von Hotspots

Hotspots sind Schaltflächen, die in Terminalsitzungen über häufig verwendeten Hostbefehlen eingeblendet werden. Wenn Sie Hotspots verwenden, können Sie die Terminalsitzung statt mit der Tastatur per Maus oder Fingerdruck steuern. Der Hotspot überträgt eine Terminaltaste oder einen Befehl zum Host. Hotspots sind standardmäßig für die Verwendung von 3270-, 5250- und VT-Befehlen konfiguriert.

Sie sind standardmäßig aktiviert und werden angezeigt, können jedoch für bestimmte Sitzungen deaktiviert oder ausgeblendet werden.

- Hotspots aktivieren

  Wählen Sie „Nein“ aus, um Hotspots in einer Sitzung zu deaktivieren.

- Hotspots anzeigen

  Wählen Sie „Nein“ aus, um Hotspots auf dem Bildschirm auszublenden. Die Hotspots sind weiterhin funktionsfähig.

Hotspots für 3270-Hosts

Hotspot	Beschreibung
PF1...PF24	Sendet die Tastenwerte PF1...PF24 zum Host
PA1, PA2 oder PA3	Sendet die Tastenwerte PA1, PA2 oder PA3 zum Host
Eingabe	Sendet die Eingabetaste an den Host
Mehr	Sendet die Löschtaste an den Host

Hotspots für 5250-Hosts

Hotspot	Beschreibung
Eingabe	Sendet die Eingabetaste an den Host
Mehr	Sendet die „Nach oben rollen“-Taste an den Host (blättert eine Seite nach unten)
PF1...PF24	Sendet die Tastenwerte PF1...PF24 zum Host

Hotspots für VT-Hosts

Hotspot	Beschreibung
F1...F20	Sendet die Tastenwerte F1...F20 zum Host

5.2.3 Konfigurieren der Bildschirmabmessungen für VT-, UTS- und T27-Hosts

Als Administrator können Sie die Anzahl der Spalten und Zeilen für VT-, UTS- und T27-Sitzungen auswählen.

1. Öffnen Sie den Bereich „Anzeige“.
2. Geben Sie unter „Abmessungen“ die Anzahl der Spalten und Zeilen an, die in jedem Bildschirm enthalten sein sollen. Der Standardwert ist 80 Spalten mal 24 Zeilen.

   Es stehen einige hostspezifische Einstellungen zur Verfügung:

   - Seiten – Wenn Sie eine Verbindung mit einem T27-Hostbildschirm herstellen, können Sie die Anzahl der anzuzeigenden Seiten festlegen. Der Standardwert ist 2.
   - Bei Hostränderung löschen – Wenn Sie eine Verbindung mit einem VT-Hostbildschirm herstellen, wählen Sie diese Option aus, um das Terminalfenster zu löschen und die Inhalte in den Scrollback-Puffer zu verschieben, wenn sich die Spaltengröße ändert.
3. Klicken Sie auf „Speichern“.

5.2.4 Festlegen von Cursoroptionen

Mit den Optionen unter „Cursor“ konfigurieren Sie die Darstellung und das Verhalten von Cursor und Lineal.

Option	Funktion...
Cursortyp	• „Unterstrichen“ zeigt den Cursor als Unterstrich an. • „Vertikaler Strich“ zeigt den Cursor als vertikalen Strich an. • „Block“ zeigt den Cursor als Block in invertierter Darstellung an.
Linealtyp	• „Vertikal“ zeigt ein vertikales Lineal an der Cursorposition an. • „Horizontal“ zeigt ein horizontales Lineal an der Cursorposition an. • „Fadenkreuz“ zeigt ein horizontales und ein vertikales Lineal an der Cursorposition an.
Cursorfarbe	Klicken Sie auf das Feld „Farbe“, um die Farbpalette zu öffnen. Wählen Sie aus der Farbpalette die gewünschte Farbe des Cursors und des Lineals aus. Alternativ dazu geben Sie die Nummer der gewünschten Hex-Farbe ein.
Cursorblinken	In der Standardeinstellung blinkt der Cursor (als Block oder Unterstrich dargestellt). Deaktivieren Sie diese Option, um den Cursor ohne Blinken anzuzeigen.

5.2.5 Festlegen von Schriftartoptionen

Verwenden Sie die folgenden Schriftartoptionen, um sicherzustellen, dass die Terminalzeichen in der gewünschten Schriftgröße und mit dem gewünschten Schriftschnitt angezeigt werden.

Option	Funktion...
Schriftgröße	• Automatisch (Standardeinstellung) – Die Schriftart wird automatisch entsprechend der Größe des Fensters skaliert. Wenn diese Option ausgewählt ist, können Sie „Pixelverhältnis beibehalten“ auswählen, sodass die Schriftgröße dynamisch angepasst wird, die Terminalanzeige jedoch nicht gestreckt oder skaliert wird, um den verfügbaren Platz zu füllen. • Fest – Geben Sie die Größe für die Anzeige des Terminalfensters in Pixel an.
Nullzeichen	Um das standardmäßige Nullzeichen vom Buchstaben O zu unterscheiden, können Sie eine der folgenden Optionen auswählen: • Standard • Null mit Schrägstrich • Null mit Punkt

5.2.6 Festlegen der Optionen des VT-Scrollback-Puffers

Der VT-Scrollback-Puffer enthält die per Bildlauf aus der Anzeige bewegten Daten, auf die der Hostcomputer nicht mehr zugreifen kann. Wenn ein Scrollback-Puffer vorhanden ist, können Sie sie mit der vertikalen Bildlaufleiste anzeigen.

Der Scrollback-Puffer ist standardmäßig aktiviert. Wenn der Scrollback-Puffer aktiviert ist, werden die Zeilen, die beim Blättern auf dem Terminalbildschirm nicht mehr zu sehen sind, in einen Puffer

geschrieben. Diese Option ist für alle Benutzer verfügbar, wenn der Administrator ihnen die Berechtigung zum Ändern der Einstellungen für die Terminalanzeige erteilt hat.

Option	Funktion...
Scrollback-Zeilenhöchstzahl	Begrenzt die Anzahl der Zeilen im Scrollback-Puffer. Die Standardeinstellung ist 500 Zeilen.
Bildschirminhalt vor dem Löschen speichern	Wenn diese Option ausgewählt ist (Standard), werden die Daten auf der Terminalanzeige beim Löschen des Bildschirminhalts (durch Sie oder den Host) in den Scrollback-Puffer verschoben. Wenn der Inhalt der Terminalanzeige nicht im Scrollback-Puffer gespeichert werden soll, deaktivieren Sie diese Option. Beim Löschen des Inhalts der Terminalanzeige werden die Daten dann verworfen.
Bildlaufbereiche speichern	Wenn für die Bildschirmanzeige ein oberer und unterer Rand definiert ist (z. B. durch einen Texteditor wie EDT bzw. TPU oder durch die DECSTBM-Funktion), wird der Bereich innerhalb dieser Ränder als Bildlaufbereich bezeichnet. Wenn diese Option deaktiviert ist, wird der Text innerhalb des Bildlaufbereichs nicht im Scrollback-Puffer gespeichert. Sollen die im Bildlaufbereich enthaltenen Daten im Scrollback-Puffer gespeichert werden, müssen Sie die Option auswählen. Hinweis: Dies kann dazu führen, dass der Anzeigespeicher sehr schnell voll wird.
Vor dem Löschen aus Zeilen speichern	Mit dieser Einstellung wird angegeben, ob Daten, die aus einem Bereich des Terminalfensters gelöscht wurden, im Bildschirmspeicher gespeichert werden.
Leerzeilen komprimieren	Wählen Sie diese Option aus, um Speicherplatz im Bildschirmspeicher freizugeben, indem mehrere Leerzeilen in eine einzige Leerzeile komprimiert werden.

5.2.7 Festlegen von Tastaturoptionen

Sie können die folgenden Tastaturoptionen festlegen:

- 3270-Optionen
- 5250-Optionen
- VT-Optionen
- T27-Optionen

3270-Optionen

- Eingabepuffer

Wenn diese Option aktiviert ist, speichert Host Access for the Cloud die in das Terminalfenster eingegebenen Zeichen in einem Pufferspeicher. Mithilfe des Eingabepuffers können Sie Ihre Eingabe auch noch fortsetzen, nachdem Sie bereits Daten an den Host gesendet haben. Ohne Eingabepuffer werden die eingegebenen Zeichen ignoriert, bis der Host weitere Daten empfangen kann.

- Textumbruch

  Wenn diese Option ausgewählt ist, wird die Funktion für den Textumbruch innerhalb eines mehrzeiligen ungeschützten Felds aktiviert. Im Modus für den Textumbruch werden einige der freien Stellen zwischen Wörtern durch Zeilenumbrüche ersetzt, sodass jede Zeile im Terminalfenster sichtbar ist und ohne horizontalen Bildlauf gelesen werden kann.

- Attention-Taste sendet

  Gibt an, was beim Drücken der ATTN-Taste gesendet wird. Die Optionen sind: Telnet-Abbruch, Ausgabeabbruch und Prozessunterbrechung.

5250-Optionen

- Eingabepuffer

  Wenn diese Option aktiviert ist, speichert Host Access for the Cloud die in das Terminalfenster eingegebenen Zeichen in einem Pufferspeicher. Mithilfe des Eingabepuffers können Sie Ihre Eingabe auch noch fortsetzen, nachdem Sie bereits Daten an den Host gesendet haben. Ohne Eingabepuffer werden die eingegebenen Zeichen ignoriert, bis der Host weitere Daten empfangen kann.

- Automatische Zurücksetzung bei Fehler

  Wenn diese Option ausgewählt ist, wird nach einem Tastaturfehler durch Drücken einer weiteren Taste der aufgetretene Fehler gelöscht. Anschließend werden die vorherigen Fehlerzeilendaten wiederhergestellt, und es wird versucht, die Tastatureingabe wie folgt auszuführen:

  Wenn der Cursor in einem gültigen Eingabefeld steht und es sich bei der Eingabe um eine Dateneingabe handelt, werden die Daten dort eingetragen, sofern sie für dieses Feld als gültige

Daten betrachtet werden (z. B. kann ein numerisches Eingabefeld nur Zahlenwerte akzeptieren).

- Wenn der Cursor in einem gültigen Eingabefeld steht und die Eingabe über eine Funktionstaste erfolgt, wird die Tastenoperation ausgeführt.
- Wenn die aktuelle Cursorposition kein gültiges Eingabefeld ist und es sich bei der Eingabe um eine Dateneingabe handelt, wird der Cursor zum nächsten gültigen Eingabefeld bewegt. Dort werden die Daten eingetragen, sofern sie für dieses Feld als gültige Daten betrachtet werden.
- Wenn die aktuelle Cursorposition kein gültiges Eingabefeld ist und die Eingabe über eine Funktionstaste erfolgt, wird der Cursor zum nächsten gültigen Eingabefeld bewegt, und die Funktionstaste wird ignoriert.
- Wenn der aktuelle Bildschirm keine gültigen Eingabefelder aufweist, wird bei jeder Tastatureingabe eine Fehlermeldung angezeigt und keine Tastatureingabe ausgeführt.

Wenn die Option deaktiviert ist, müssen Sie die Taste zum Zurücksetzen drücken, um die Fehlermeldung aus der Fehlerzeile zu löschen. Erst dann können Sie die Dateneingabe fortsetzen.

Diese Option ist standardmäßig nicht aktiviert.

- Feldprüfungen für PF-Taste übergehen

  Wählen Sie diese Option aus, um zuzulassen, dass PF-Tasten von eingeschränkten Feldern an den Host gesendet werden können. Diese Option ist standardmäßig deaktiviert.

VT-Optionen

- Rücktaste sendet

  Konfiguriert die Funktion, die die Rücktaste sendet. Auf der Tastatur des VT-Terminals kann die Rückwärtspfeiltaste `(<x)` so konfiguriert werden, dass entweder ein Löschzeichen (ASCII 127) oder ein Rücktastenzeichen (ASCII 8) gesendet wird.

- Lokales Echo (VT)

  Wenn diese Option ausgewählt ist, werden über die Tastatur eingegebene Zeichen auf dem Bildschirm angezeigt. Diese Option ist standardmäßig ausgewählt, da die meisten Hosts für empfangene Zeichen ein Echosignal aussenden.

- Pfeiltasten

  Hier wird festgelegt, welche Zeichen durch die vier Pfeiltasten (sowohl im Bearbeitungs- als auch im numerischen Tastenfeld) übertragen werden. Diese Einstellung wird normalerweise vom Host festgelegt. Im Allgemeinen sollten Sie dies auf „Normal“ festgelegt lassen.

  Wenn die Pfeiltasten nicht richtig funktionieren, wurde diese Option möglicherweise beim anormalen Beenden eines Hostprogramms auf „Anwendung“ gesetzt gelassen. Probleme mit

den Pfeiltasten sollten durch Zurücksetzen dieser Einstellung auf „Normal“ behoben werden können.

- Numerisches Tastenfeld

  Hier wird festgelegt, welche Zeichen durch die Tasten des numerischen Tastenfelds übertragen werden. Diese Einstellung wird normalerweise vom Host festgelegt. Es wird empfohlen, die Einstellung „Numerisch“ beizubehalten.

  Wenn die Nummern- oder PF-Tasten nicht richtig funktionieren, wurde diese Option möglicherweise nach dem anormalen Beenden eines Hostprogramms fälschlicherweise auf „Anwendung“ gesetzt gelassen. Probleme mit dem numerischen Tastenfeld sollten durch Zurücksetzen dieser Einstellung auf „Numerisch“ behoben werden können.

T27-Optionen

- Kleinschreibung aktivieren (T27)

  Aktiviert die Anzeige von Kleinbuchstaben und Großbuchstaben auf dem Bildschirm. Standardeinstellung. Wenn diese Option deaktiviert ist, werden nur Großbuchstaben angezeigt.

5.2.8 Terminaleinstellungen

Je nach Hosttyp können die Terminaleinstellungen variieren.

3270- und 5250-Terminaleinstellungen

- Hostzeichensatz

  Wählen Sie den 3270- oder 5250-Hostzeichensatz aus, der verwendet werden soll. Bei dieser Einstellung wird für die Konvertierung von Hostzeichen (EBCDIC) in PC-Zeichen (ANSI) eine Konvertierungstabelle ausgewählt. Diese Einstellung sollte mit dem nationalen Zeichensatz übereinstimmen, der von Ihrem Hostsystem verwendet wird. Falls sie nicht übereinstimmt, könnten einige Zeichen, z. B. Modifikationszeichen (Betonungszeichen), falsch angezeigt werden. Schlagen Sie in Ihrer Hostdokumentation die Definitionen der in den betreffenden Zeichensätzen enthaltenen Zeichen nach. Der Standardwert ist Englisch (US) (037).

- Erweiterter nationaler Grafikzeichensatz (nur 3270)

  Wenn diese Option ausgewählt ist (Standardeinstellung), stehen im konfigurierten nationalen Zeichensatz Zusatzzeichen zur Verfügung. Weitere Informationen finden Sie in der Dokumentation zum Hostsystem..

VT-Terminaleinstellungen

- Terminaltyp (VT)

Gibt an, welches Terminal emuliert werden soll. Diese Auswahl hat Auswirkungen auf die mit dem numerischen Tastenfeld erzeugten Codes, die Interpretation der Steuerfunktionen und die Reaktion auf Terminalkennungsanforderungen.

- Terminalkennung (VT)

  Diese Einstellung legt fest, welche Antwort Host Access for the Cloud nach einer primären Geräteattributanforderung an den Host sendet. Anhand der Antwort kann der Host erkennen, welche Terminalfunktionen ausgeführt werden können. Diese Einstellung ist unabhängig von der Einstellung für den Terminaltyp. Wenn sie auf den Standardwert von Reflection festgelegt ist, werden auf eine Anforderung der primären Geräteattribute die von Host Access for the Cloud unterstützten Funktionen gemeldet. Wenn Ihr Host eine spezifische Terminalkennung erfordert, wählen Sie in der Liste einen anderen Wert aus.

- Neue Zeile (VT)

  Aktivieren Sie diese Option, damit beim Drücken der Eingabetaste eine Zeilenschaltung und ein Zeilenvorschub gesendet werden. Wenn Host Access for the Cloud ein Zeilenvorschub-, Seitenvorschub- oder Vertikaltabulatorzeichen empfängt, wird der Cursor in die erste Spalte der nächsten Zeile gesetzt. Wenn diese Option deaktiviert ist (Standardeinstellung), sendet die Eingabetaste nur eine Zeilenschaltung. Wird ein Zeilenvorschub-, Seitenvorschub- oder Vertikaltabulatorzeichen empfangen, wird der Cursor in der Spalte, in der er sich befindet, um eine Zeile nach unten geführt. Wenn Anzeigezeilen überschrieben werden sollen, müssen Sie diese Option auswählen (der Host sendet dann mit der Zeilenschaltung keinen Zeilenvorschub). Wenn die Option Neue Zeile ausgewählt ist, aber der Host nicht bei jeder Zeilenschaltung einen Zeilenvorschub erwartet, werden die Zeilen auf der Anzeige mit zweizeiligem Abstand angezeigt.

T27-Terminaleinstellungen

- Hostzeichensatz (T27)

  Durch Verwenden dieser Option können Sie die Umwandlung der Zeichen vom Host auf dem Bildschirm angeben. Wählen Sie die Sprache aus, die zum Umwandeln der vom Host empfangenen Zeichen verwendet wird, bevor diese auf dem lokalen Computer angezeigt werden. Die Standardeinstellung ist „Keine Umwandlung“.

5.2.9 Festlegen weiterer Anzeigeoptionen

Option	Funktion...
Spaltentrennzeichen-Stil (5250)	Mit dieser Option legen Sie fest, welche Zeichen (sofern vorhanden) zum Darstellen von Spaltentrennzeichen in 5250-Terminalsitzungen verwendet werden sollen. Die Optionen sind: • Punkte – Spalten werden durch Punkte getrennt. Standardeinstellung. • Vertikale Striche – Spalten werden durch vertikale Linien getrennt. • Keine – Zum Trennen von Spalten werden keine Zeichen verwendet.
Unterstreichung von Eingabefeldern (3270, 5250)	Sie können festlegen, wie die Unterstreichung von Hosteingabefeldern erfolgt: • Host steuert Unterstreichung (Standard) • Eingabefelder immer unterstreichen • Eingabefelder nie unterstreichen
Statuszeile (VT)	Aktivieren einer Statuszeile unten in der Anzeige. • Die Einstellung „Kein“ deaktiviert die Statuszeile. (Standard) • Die Einstellung „Indikator“ zeigt die Seite, die Cursorposition und den Druckerstatus an. • Die Einstellung „Schreibbar durch Host“ zeigt Informationen der Hostanwendung in der Statuszeile an.
Pixelverhältnis beibehalten	Wählen Sie diese Option aus, um die Proportionen des Hostbildschirms unabhängig von der Größe des Browserfensters beizubehalten. Die Proportionen beschreiben das proportionale Verhältnis zwischen der Breite und der Höhe eines Bildes.
OIA anzeigen (3270, 5250)	Wählen Sie diese Option aus, um Vorgangs- und Statusmeldungen im Operatorinformationsfeld (OIA, Operator Information Area) im unteren Terminalfensterbereich anzuzeigen. Die OIA-Anzeige ist standardmäßig aktiviert.
Statuszeile anzeigen (ALC)	Aktiviert eine Statuszeile unten in der Anzeige.
Mausklick auf Fenster ignorieren aktivieren	Wenn das Terminalfenster durch einen Mausklick aktiviert wird, geben Sie mit dieser Option an, ob Aktionen wie das Aktualisieren der Terminal-Cursorposition, das Aufheben der

	Auswahl oder das Ausführen eines Hotspots ebenfalls durchgeführt werden. Diese Aktionen werden standardmäßig nicht durchgeführt.
Automatischer Umbruch (VT)	Wenn dieses Kontrollkästchen aktiviert ist, werden Zeichen am rechten Rand automatisch umbrochen und auf der nächsten Zeile fortgesetzt. Wenn das Kontrollkästchen deaktiviert ist, werden Zeichen beim Erreichen des rechten Rands der Anzeige nicht umbrochen. Das Zeichen am rechten Rand wird durch neue Zeichen überschrieben, bis ein Wagenrücklaufzeichen eingegeben wird.

5.3 Tasten zuordnen

5.3.1 Tasten zuordnen

Sie können Tastenkombinationen definieren, über die während einer Sitzung jede zuweisbare Aktion ausgeführt werden kann. Auf der Einstellungsseite „Tastenbelegungen“ können Sie die Standardtastaturbelegung für jeden Hosttyp und die zugeordneten benutzerdefinierten Tasten (in Fettschrift angegeben) für die jeweilige Sitzung anzeigen.

Informationen zu den verschiedenen Hosttastaturbelegungen finden Sie unter Hosttastaturbelegung.

Zuordnen von Tasten als Administrator und als Endbenutzer

Es gibt einige Unterschiede im Verhalten zwischen dem Administrator und dem Endbenutzer bei der Zuordnung von Tasten.

- Endbenutzer können Tastenbelegungen nur hinzufügen oder ändern, wenn ihnen vom Administrator im Bereich „Regeln für Benutzereinstellungen“ die entsprechende Berechtigung erteilt wurde.
- Alle vom Administrator vorgenommenen Änderungen werden für den Endbenutzer nicht erkennbar zusammen mit den standardmäßigen Hosttastenbelegungen angezeigt. Nach Erteilung der Berechtigung kann der jeweilige Benutzer alle Zuordnungen unabhängig von den vom Administrator vorgenommenen Änderungen ändern, hinzufügen oder löschen. Beim Wiederherstellen von Tastenbelegungen werden die Tasten jedoch nur auf den geänderten Status zurückgesetzt, der vom Administrator für die aktuelle Sitzung erstellt wurde.

Hinzufügen oder Ändern von zugeordneten Tasten

1. Klicken Sie in der Symbolleiste auf „Einstellungen“.
2. Öffnen Sie im linken Navigationsbereich den Bereich „Tastenbelegungen“. Die zugeordneten Tasten für den Hosttyp für die jeweilige Verbindung werden angezeigt.
3. So fügen Sie eine neue Tastenbelegung hinzu:

   - Klicken Sie auf . Sie können die gewünschte Tastenfolge eingeben oder die Tastatur verwenden. Wechseln Sie mit zwischen den beiden Optionen.
   - Wählen Sie aus der Dropdown-Liste „Aktion“ die Aktion aus, die Sie der Tastenauswahl zuordnen möchten. Wenn Sie „Text senden“ auswählen, geben Sie im Feld „Wert“ die Zeichenkette ein, die Sie an den Host senden möchten. Wählen Sie bei Auswahl von „Makro ausführen“ ebenso das Makro aus, das durch die Tastenkombination ausgelöst werden soll. Sie müssen zunächst das Makro erstellen, damit Sie es der Aktion „Makro ausführen“ zuordnen können.

     Die Aktion „Text senden“ unterstützt das Zuordnen von Zeichen mit Codes kleiner oder gleich `0xFFFF` als Unicode-Escape-Sequenzen. Die Escape-Sequenz beginnt mit `\u` gefolgt von genau vier Hexadezimalziffern. Unicode-Escape-Sequenzen können in beliebige Zeichenketten eingebettet werden. So wird beispielsweise dieses eingebettete `\u0045` als dieses eingebettete E interpretiert, da 45 der Hexadezimalcode für den Buchstaben E ist.

     Für die Übergabe der Unicode-Escape-Sequenzen an den Host stellen Sie der Sequenz einen Backslash voran. Soll beispielsweise der Buchstabe \u001C an den Host gesendet werden, belegen Sie eine Taste mit `\\u001C`. Beim Drücken dieser Taste wandelt Host Access for the Cloud dies in die Zeichenkette `\u001C` um und sendet die 6 Zeichen der daraus entstehenden Zeichenkette an den Host.

     Mit der Aktion „Deaktivieren“ wird die entsprechende Taste funktionslos. Beim Drücken der Taste wird keine Aktion gestartet. Dies unterscheidet sich von der Aktion „Unmap“ (Zuordnung aufheben), bei der zwar die Tastenbelegung entfernt wird, die Tastenkombination im Browser jedoch beibehalten wird, sofern sie definiert ist.
   - Klicken Sie auf das blaue Häkchen, um die Zuordnung zu bestätigen und die Tastaturbelegung zur Sitzung hinzuzufügen.

4. So ändern Sie eine vorhandene Belegung:

   Wählen Sie die Zeile mit der zu ändernden Taste aus.

   Führen Sie die Schritte zum Hinzufügen einer neuen Tastenbelegung aus und klicken Sie auf , um die neue Tastenbelegung zu speichern. Alternativ können Sie neben die geänderte Zeile klicken. Dadurch wird die Änderung gespeichert. Alle neuen und geänderten Tastenbelegungen werden in Fettschrift angezeigt. Sie können die ursprüngliche Tastenbelegung jederzeit wiederherstellen, indem Sie auf klicken.

Filtern der Liste

Im Feld „Filter“ können Sie auf einfache Weise nur die gewünschten Belegungen anzeigen. Der Filter basiert auf Schlüsselwörtern und gilt für alle Spalten der Tabelle. Wenn Sie beispielsweise „Text senden“ im Feld „Filter“ eingeben, werden nur die der Aktion „Text senden“ zugeordneten Tasten angezeigt.

Über die Option „Nur geänderte Zuordnungen anzeigen“ können Sie nur die Belegungen anzeigen, die zuvor geändert wurden.

Folgendes ist zu beachten:

- Zuordnen der rechten und der linken Zusatztaste zu einzelnen Aktionen

  Sie können die rechte und die linke Zusatztaste einzelnen Aktionen zuordnen. Wenn sie jedoch mit anderen Tasten kombiniert werden, wird zwischen der rechten und der linken Taste nicht unterschieden. Die linke Alt-Taste kann beispielsweise Aktion-A zugeordnet werden und die rechte Alt-Taste zu Aktion-B. Alt links+H wird jedoch als Alt+H gespeichert, sodass sowohl Alt links+H als auch Alt rechts+H mit ein und derselben zugeordneten Aktion verknüpft sind.

- Tastenkombinationen und Kopier- und Einfügevorgänge

  Auch für Kopier- und Einfügevorgänge werden verschiedene Tastenkombinationen verwendet. So wird beispielsweise auf einem VT-Hostbildschirm über die Tastenkombination Strg+Umschalt+A die Aktion „Alles auswählen“ ausgelöst. Eine Liste der Tastenaktionen zum Kopieren/Einfügen finden Sie unter „Bearbeiten des Bildschirms“.

- Tastenkombinationen und Browser

  Browser verwenden Tastenkombinationen, um Zeitaufwand und Mausklicks zu reduzieren. Dies sollte bei der Zuordnung von Tastenkombinationen berücksichtigt werden. Unter „Handy Keyboard Shortcuts“ (Nützliche Tastenkombinationen) erhalten Sie einen Überblick über die in den verschiedenen Browsern verwendeten Tastenkombinationen. In den meisten Fällen haben die Host Access for the Cloud-Tastenzuordnungen eine höhere Rangordnung als die Tastenkombinationen des Browsers. Wenn dies für eine bestimmte Tastenkombination nicht dem gewünschten Verhalten entspricht, können Sie für den jeweiligen Fall „Unmap“ (Zuordnung aufheben) in der Aktionsliste wählen, um die Zuordnung der Tastenkombination aufzuheben. Auf diese Weise kann das Tastenereignis an den Browser weitergeleitet werden.

5.3.2 Hosttastaturbelegung

Die folgenden Tabellen zeigen die Standardtasten, Tastennamen und die Beschreibungen für die verschiedenen Hosttastaturbelegungen.

- IBM 3270-Tastaturbelegung
- IBM 5250-Tastaturbelegung
- VT-Tastaturbelegung
- UTS-Tastaturbelegung
- T27-Tastaturbelegung
- ALC-Tastaturbelegung

IBM 3270-Tastaturbelegung

Tasten	Zuordnung	Beschreibung
Strg+F1	Abruf	Sendet die Abruftaste an den Host
Umschalt+Tabulator	Rücktabulator	Bewegt den Cursor in das vorherige ungeschützte Feld
Strg+F2	Löschen	Entfernt den Bildschirminhalt und sendet die Löschtaste an den Host
Alt+Pfeil nach links	Cursor nach links – doppelt	Bewegt den Cursor um zwei Positionen nach links
Alt+Pfeil nach rechts	Cursor nach rechts – doppelt	Bewegt den Cursor um zwei Positionen nach rechts
Strg+F3	Cursorauswahl	Simuliert eine Lightpen-Auswahl im aktuellen Feld
Alt+Entf	Wort löschen	Löscht drei Zeichen aus dem aktuellen Feld
Strg+5	Duplizieren	Fügt das DUP-Zeichen an der Cursorposition ein
Eingabe	Eingabe	Sendet die Eingabetaste an den Host
Ende	Feldende löschen	Löscht alle Daten ab der aktuellen Cursorposition bis zum aktuellen Feldende
Alt+F5	Eingabe löschen	Löscht alle Daten aus allen ungeschützten Feldern des aktuellen Bildschirms
Strg+Alt+F	Feldtrennzeichen	Schaltet die Anzeige der Feldtrennzeichen ein bzw. aus
Strg+6	Feldmarkierung	Fügt das Feldmarkierungszeichen an der Cursorposition ein
Pos1	Pos1	Bewegt den Cursor in das erste ungeschützte Feld auf dem Bildschirm
Einf	Einfügen	Ändert den Einfügemodus
Umschalt+Eingabe	Neue Zeile	Bewegt den Cursor in das nächste ungeschützte Feld

Tasten	Zuordnung	Beschreibung
Strg+1	PA1	Sendet die PA1-Taste an den Host
Bild nach oben	PA1	Sendet die PA1-Taste an den Host
Strg+2	PA2	Sendet die PA2-Taste an den Host
Bild nach unten	PA2	Sendet die PA2-Taste an den Host
Strg+3	PA3	Sendet die PA3-Taste an den Host
F1 – F10	PF1 – PF10	Sendet die PF1, PF2...PF10-Tasten an den Host
Alt+1 oder F11	PF11	Sendet die PF11-Taste an den Host
Alt + 2 oder F12	PF12	Sendet die PF12-Taste an den Host
Umschalt+F1	PF13	Sendet die PF13-Taste an den Host
Umschalt+F2	PF14	Sendet die PF14-Taste an den Host
Umschalt+F3	PF15	Sendet die PF15-Taste an den Host
Umschalt+F4	PF16	Sendet die PF16-Taste an den Host
Umschalt+F5	PF17	Sendet die PF17-Taste an den Host
Umschalt+F6	PF18	Sendet die PF18-Taste an den Host
Umschalt+F7	PF19	Sendet die PF19-Taste an den Host
Umschalt+F8	PF20	Sendet die PF20-Taste an den Host
Umschalt+F9	PF21	Sendet die PF21-Taste an den Host
Umschalt+F10	PF22	Sendet die PF22-Taste an den Host
Alt+3	PF23	Sendet die PF23-Taste an den Host
Umschalt+F11	PF23	Sendet die PF23-Taste an den Host
Alt+4	PF24	Sendet die PF24-Taste an den Host
Umschalt+F12	PF24	Sendet die PF24-Taste an den Host
Strg+P	Druck	Sendet den Bildschirminhalt an den Drucker
Esc	Zurücksetzen	Setzt Tastaturfehler zurück

Tasten	Zuordnung	Beschreibung
Strg+S	Systemanforderung	Sendet die SYSTEM REQUEST-Taste an den Host

IBM 5250-Tastaturbelegung

Tasten	Zuordnung	Beschreibung
Esc	Abruf	Sendet die Abruftaste an den Host
Strg+F2	Löschen	Entfernt den Bildschirminhalt und sendet die Löschtaste an den Host
Strg+F3	Cursorauswahl	Simuliert eine Lightpen-Auswahl im aktuellen Feld
Strg+Rücktaste	Rückschritt mit Löschen	Bewegt den Cursor um eine Position nach links
Strg+5	Duplizieren	Fügt das DUP-Zeichen an der Cursorposition ein
Strg+Ende	Feldende	Bewegt den Cursor an das Feldende
Ende	Feldende löschen	Löscht alle Daten ab der aktuellen Cursorposition bis zum aktuellen Feldende
Alt+Ende	Eingabe löschen	Löscht alle Daten aus allen ungeschützten Feldern des aktuellen Bildschirms
Alt+F5	Eingabe löschen	Löscht alle Daten aus allen ungeschützten Feldern des aktuellen Bildschirms
Strg+Eingabetaste	Feldende	Bewegt den Cursor aus einem Eingabefeld heraus
Nt+Minus	Feldende Minus	Bewegt den Cursor aus einem Feld für numerische Daten mit oder ohne Vorzeichen heraus und fügt an der letzten Position eines Feldes mit Vorzeichen ein Minuszeichen (-) ein bzw. ändert die letzte Position in einem Feld ohne Vorzeichen in einen Buchstaben, der dem System mitteilt, dass dieses Feld einen negativen Wert enthält.
Strg+Minus	Feldende Minus	Bewegt den Cursor aus einem Feld für numerische Daten mit oder ohne Vorzeichen heraus und fügt an der letzten Position eines Feldes mit Vorzeichen ein Minuszeichen (-) ein bzw. ändert die

Tasten	Zuordnung	Beschreibung
		letzte Position in einem Feld ohne Vorzeichen in einen Buchstaben, der dem System mitteilt, dass dieses Feld einen negativen Wert enthält.
Nt+Plus	Feldende Plus	In einem Feld für numerische Daten mit Vorzeichen wird der Cursor in das nächste Feld bewegt, wobei ein an der letzten Position stehendes Minuszeichen entfernt wird. In einem Feld für numerische Daten ohne Vorzeichen bewegt diese Funktion den Cursor in das nächste Feld und ändert die letzte Position in einen Buchstaben, der dem System mitteilt, dass dieses Feld einen positiven Wert enthält.
Strg+Plus	Feldende Plus	In einem Feld für numerische Daten mit Vorzeichen wird der Cursor in das nächste Feld bewegt, wobei ein an der letzten Position stehendes Minuszeichen entfernt wird. In einem Feld für numerische Daten ohne Vorzeichen bewegt diese Funktion den Cursor in das nächste Feld und ändert die letzte Position in einen Buchstaben, der dem System mitteilt, dass dieses Feld einen positiven Wert enthält.
Strg+6	Feldmarkierung	Fügt das Feldmarkierungszeichen an der Cursorposition ein
Strg+H	Hilfe	Sendet die Hilfetaste an den Host
Alt+F7	Hexadezimalmodus	Versetzt das Terminal in den Hexadezimalmodus
Pos1	Pos1	Bewegt den Cursor in das erste ungeschützte Feld auf dem Bildschirm
Einf	Einfügen	Ändert den Einfügemodus
Umschalt+Eingabe	Neue Zeile	Bewegt den Cursor in das nächste ungeschützte Feld

Tasten	Zuordnung	Beschreibung
Strg+1	PA1	Sendet die PA1-Taste an den Host
Strg+2	PA2	Sendet die PA2-Taste an den Host
Strg+3	PA3	Sendet die PA3-Taste an den Host
F1 – F11	PF1 – PF11	Sendet die PF1, PF2....PF11-Tasten an den Host
Alt+1	PF11	Sendet die PF11-Taste an den Host
Alt+2	PF12	Sendet die PF12-Taste an den Host
F12	PF12	Sendet die PF12-Taste an den Host
Umschalt+1	PF13	Sendet die PF13-Taste an den Host
Umschalt+F2...F10	PF14–PF22	Sendet die PF14- bis PF22-Tasten an den Host
Alt+3	PF23	Sendet die PF23-Taste an den Host
Umschalt+F11	PF23	Sendet die PF23-Taste an den Host
Alt+4	PF24	Sendet die PF24-Taste an den Host
Umschalt+F12	PF24	Sendet die PF24-Taste an den Host
Strg+P	Drucken	Sendet den Bildschirminhalt an den Drucker
Strg	Zurücksetzen	Setzt Tastaturfehler zurück
Bild nach oben	Nach unten blättern	Sendet die Nach-unten-blättern-Taste an den Host
Bild nach unten	Nach oben blättern	Sendet die Nach-oben-blättern-Taste an den Host
Strg+Pos1	Feldanfang	Bewegt den Cursor an den Feldanfang
Strg+S	Systemanforderung	Sendet die SYSTEM REQUEST-Taste an den Host

VT-Tastaturbelegung

Tasten	Zuordnung	Beschreibung
Strg+Untbr	Unterbrechungstaste	Sendet die Unterbrechungstaste an den Host
Strg+Eingabe	Eingabe	Sendet die Eingabetaste an den Host
Alt+F1	F1	Sendet die F1-Taste an den Host
Strg+F1...F10	F11–F20	Sendet die F11- bis F20-Tasten an den Host
Pos1	Suchen	Sendet die Suchen-Taste an den Host
F1	Anhalten	Sendet die Anhalten-Taste an den Host
Pause	Anhalten	Sendet die Anhalten-Taste an den Host
Einfg	Einfügen	Sendet die Einfügen-Taste an den Host
Strg+Einfg	Nt0	Sendet die Nt0-Taste des numerischen Tastenfelds an den Host
Strg+Ende	Nt1	Sendet die Nt1-Taste des numerischen Tastenfelds an den Host
Strg+Pfeil nach unten	Nt2	Sendet die Nt2-Taste des numerischen Tastenfelds an den Host
Strg+Bild nach unten	Nt3	Sendet die Nt3-Taste des numerischen Tastenfelds an den Host
Strg+Pfeil nach links	Nt4	Sendet die Nt4-Taste des numerischen Tastenfelds an den Host
Strg+Löschen	Nt5	Sendet die Nt5-Taste des numerischen Tastenfelds an den Host
Strg+Pfeil nach rechts	Nt6	

Tasten	Zuordnung	Beschreibung
		Sendet die Nt6-Taste des numerischen Tastenfelds an den Host
Strg+Pos1	Nt7	Sendet die Nt7-Taste des numerischen Tastenfelds an den Host
Strg+Pfeil nach oben	Nt8	Sendet die Nt8-Taste des numerischen Tastenfelds an den Host
Strg+Bild nach oben	Ziffernblock 9	Sendet die Nt9-Taste des numerischen Tastenfelds an den Host
Strg+Alt-Plus	NtKomma	Sendet die NtKommataste des numerischen Tastenfelds an den Host
Strg+Plus	NtMinus	Sendet die NtMinustaste des numerischen Tastenfelds an den Host
Strg+Dezimal	NtPunkt	Sendet die NtPunkt-Taste des numerischen Tastenfeldes an den Host
Strg+Löschen	NtPunkt	Sendet die NtPunkt-Taste des numerischen Tastenfeldes an den Host
Strg+Alt+Pfeil nach oben	Zeile nach oben	Wird im Scrollback-Puffer eine Zeile nach oben verschoben
Strg+Alt+Pfeil nach unten	Zeile nach unten	Wird im Scrollback-Puffer eine Zeile nach unten verschoben
Bild nach unten	Nächster	Sendet die „Nächster-Bildschirm“-Taste an den Host
Strg+Pause	PF1	Sendet die PF1-Taste an den Host
Strg+Dividieren	PF2	Sendet die PF2-Taste an den Host
Strg+Multiplizieren	PF3	Sendet die PF3-Taste an den Host

Tasten	Zuordnung	Beschreibung
Strg+Minus	PF4	Sendet die PF4-Taste an den Host
Bild nach oben	Vorherig	Sendet die „Vorhergehender Bildschirm“-Taste an den Host.
Löschen	Entfernen	Sendet die Löschfunktion-Taste an den Host
Ende	Auswählen	Sendet die Selektieren-Taste an den Host.
Umschalt+F6...F10	UDK6–10	Sendet die Benutzertasten 6 bis 10 an den Host
Umschalt+Strg+F1–F10	UDK11–20	Sendet die Benutzertasten 11 bis 20 an den Host

UTS-Tastaturbelegung

Tasten	Zuordnung	Beschreibung
F4	Änderungsbit löschen	Sendet die CLEARCHANGEBIT-Taste an den Host
NtEingabe	Zeilenschaltung	Sendet eine Zeilenschaltung an den Host
Strg+Bild nach unten	Anzeigeende löschen	Löscht den Text ab der Cursorposition bis zum Anzeigeende
Strg+Bild nach oben	Anzeigeende/FCC löschen	Löscht alle Daten (einschließlich FCC-Informationen) von der Cursorposition bis zum Anzeigeende.
Strg+Ende	Feldende löschen	Löscht den Text ab der Cursorposition bis zum Feldende
Strg+Umschalt+Ende	Zeilenende löschen	Löscht den Text ab der Cursorposition bis zum Zeilenende
F7	FCC löschen	Löscht das Feldsteuerungszeichen.
Strg+Pos1	Pos1 löschen	Sendet die CLEAR_HOME-Taste an den Host
Strg+H	Spaltentrennzeichen rechts	Sendet die COLUMN_SEP_RIGHT-Taste an den Host
Strg+F1	Steuerungsseite	Sendet die CONTROL_PAGE-Taste an den Host
Nt2	Cursor nach unten	Bewegt den Cursor eine Zeile nach unten
Nt4	Cursor nach links	Bewegt den Cursor um eine Spalte nach links
Nt6	Cursor nach rechts	Bewegt den Cursor um eine Spalte nach rechts
Nt8	Cursor nach oben	Bewegt den Cursor eine Zeile nach oben

Tasten	Zuordnung	Beschreibung
Löschen	In Zeile löschen	Sendet die DELETE_IN_LINE-Taste an den Host
Strg+Löschen	Auf Seite löschen	Sendet die DELETE_IN_PAGE-Taste an den Host
Strg+Umschalt+Löschen	Zeile löschen	Löscht die Zeile an der Cursorposition
Strg+Pfeil nach unten	Zeile duplizieren	Dupliziert die Zeile an der Cursorposition
F8	FCC aktivieren	Aktiviert das Feldsteuerungszeichen
Nt+-	Anzeigeende und übertragen	Sendet die EOD_AND_TRANSMIT-Taste an den Host
Umschalt+Ende	Feldende	Bewegt den Cursor an das Feldende
Ende	Zeilenende	Bewegt den Cursor an das Zeilenende
Strg+Pfeil nach rechts	Seitenende	Bewegt den Cursor an das Seitenende
Umschalt+Leertaste	Zeichen löschen	Löscht das Zeichen an der Cursorposition
Strg+Umschalt+E	Euro-Zeichen	Sendet das Eurozeichen an den Host
Strg+1–Strg+9	F1–F9	Sendet die F1- bis F9-Tasten an den Host
Strg+0	F10	Sendet die F10-Taste an den Host
Strg+-	F11	Sendet die F11-Taste an den Host
Strg+=	F12	Sendet die F12-Taste an den Host
Strg+Q	F13	

Tasten	Zuordnung	Beschreibung
		Sendet die F13-Taste an den Host
STRG+W	F14	Sendet die F14-Taste an den Host
Strg+E	F15	Sendet die F15-Taste an den Host
Strg+R	F16	Sendet die F16-Taste an den Host
Strg+T	F17	Sendet die F17-Taste an den Host
Strg+Y	F18	Sendet die F18-Taste an den Host
Strg+U	F19	Sendet die F19-Taste an den Host
Strg+I	F20	Sendet die F20-Taste an den Host
Strg+O	F21	Sendet die F21-Taste an den Host
Strg+P	F22	Sendet die F22-Taste an den Host
Umschalttaste+F3	FF	Sendet einen Papiervorschub an den Host
F9	FCC erzeugen	Erzeugt ein Feldsteuerungszeichen
Pos1	Pos1	Bewegt den Cursor in das erste Feld in der Anzeige
Strg+Umschalt+Leertaste	In Zeile einfügen	Sendet die INSERT_IN_LINE-Taste an den Host
Ctrl+Leertaste	Auf Seite einfügen	Sendet die INSERT_IN_PAGE-Taste an den Host
Strg+Umschalt+Einfg	Zeile einfügen	Fügt eine neue Zeile in den Bildschirmspeicher ein

Tasten	Zuordnung	Beschreibung
Einf	Einfügemodus	Ändert den Einfügemodus
F5	FCC suchen	Deaktiviert die Feldsteuerungszeichen und wechselt zum ersten Zeichen des nächsten Felds rechts vom Cursor
F3	Warten-Meldung	Sendet die MESSAGE_WAIT-Taste an den Host
Umschalttaste+F2	Neue Zeile	Bewegt den Cursor in eine neue Zeile
NtUmschalt+2	Nächstes Feld	Bewegt den Cursor in das nächste Feld
NtUmschalt+4	Nächstes Feld	Bewegt den Cursor in das nächste Feld
Bild nach unten	Bild nach unten	Sendet die Bild-nach-unten-Taste an den Host
Bild nach oben	Bild nach oben	Sendet die Bild-nach-oben-Taste an den Host
NtUmschalt+6	Vorheriges Feld	Bewegt den Cursor in das vorherige Feld
NtUmschalt+8	Vorheriges Feld	Bewegt den Cursor in das vorherige Feld
Löschen	SOE-Zeichen	Sendet das SOE-Zeichen an den Host
F12	SOE-Zeichen	Sendet das SOE-Zeichen an den Host
Strg+Löschen	Tab setzen	Sendet die SET_TAB-Taste an den Host
Strg+Tabulator	Tab setzen	Sendet die SET_TAB-Taste an den Host
Umschalt+Pos1	Feldanfang	Bewegt den Cursor an den Feldanfang

Tasten	Zuordnung	Beschreibung
Strg+Pfeil nach links	Zeilenanfang	Bewegt den Cursor an den Zeilenanfang.
Strg+[	Systemmodus	Sendet die SYSTEM_MODE-Taste an den Host
Strg+J	Spaltentrennzeichen ändern	Ändert das Spaltentrennzeichen
Strg+F12	Piepton für Warten-Meldung ändern	Sendet die TOGGLEMSGWAITBEEP-Taste an den Host
Strg+L	Durchstreichen ändern	Ändert den Durchstreichungsmodus
Strg+K	Unterstreichen ändern	Ändert den Unterstreichungsmodus
Strg+Eingabetaste	Übertragen	Überträgt den Anzeigeinhalt an den Host
ScrollLock	Übertragen	Überträgt den Anzeigeinhalt an den Host
Nt++	Übertragen	Überträgt den Anzeigeinhalt an den Host
NtStrg+	Übertragen	Überträgt den Anzeigeinhalt an den Host
Esc	Seite „Entsperren“	Sendet die UNLOCK-Taste an den Host
Strg+]	Workstationmodus	Sendet die WORKSTATION_MODE-Taste an den Host

T27-Tastaturbelegung

Tasten	Zuordnung	Beschreibung
Rücktaste	Rücktaste	Bewegt den Cursor um eine Spalte nach links
Umschalt+Tab	Rücktabulator	Bewegt den Cursor in das vorherige Feld
Strg+Entf	Zeilenende löschen	Löscht den Text ab der Cursorposition bis zum Zeilenende
Umschalt+Pos1	Seite löschen Pos1	Löscht die Seite und setzt den Cursor an die Ausgangsposition
Strg links	Steuerungsseite	Setzt die Sitzung in den Steuerungsmodus
Pfeil nach unten	Cursor nach unten	Bewegt den Cursor eine Zeile nach unten
Pfeil nach links	Cursor nach links	Bewegt den Cursor um eine Spalte nach links
Pfeil nach rechts	Cursor nach rechts	Bewegt den Cursor um eine Spalte nach rechts
Pfeil nach oben	Cursor nach oben	Bewegt den Cursor eine Zeile nach oben
Strg+Nach links	Cursor Wort links	Bewegt den Cursor zum vorherigen Wort
Strg+Nach rechts	Cursor Wort rechts	Bewegt den Cursor zum nächsten Wort
Strg+D	Zeile löschen	Löscht die Zeile an der Cursorposition
Strg+Ende	Zeilenende	Bewegt den Cursor an das Zeilenende
Ende	Seitenende	Bewegt den Cursor in das letzte Feld auf der Seite
Umschalt+Strg+E	Euro-Zeichen	Sendet das Eurozeichen an den Host
Pos1	Pos1	

Tasten	Zuordnung	Beschreibung
		Bewegt den Cursor in das erste Feld in der Anzeige
Einf	Einfügemodus	Setzt die Sitzung in den Einfügemodus
Strg+I	Zeile einfügen	Fügt eine neue Zeile in den Bildschirmspeicher ein
Strg+1	PF1	Sendet die PF1-Taste an den Host
Strg+10	PF10	Sendet die PF10-Taste an den Host
Strg+2	PF2	Sendet die PF2-Taste an den Host
Strg+3	PF3	Sendet die PF3-Taste an den Host
Strg+4	PF4	Sendet die PF4-Taste an den Host
Strg+5	PF5	Sendet die PF5-Taste an den Host
Strg+6	PF6	Sendet die PF6-Taste an den Host
Strg+7	PF7	Sendet die PF7-Taste an den Host
Strg+8	PF8	Sendet die PF8-Taste an den Host
Strg+9	PF9	Sendet die PF9-Taste an den Host
Bild nach unten	Bild nach unten	Zeigt die nächste Seite an
Bild nach oben	Bild nach oben	Zeigt die vorherige Seite an
Strg+E	ETX festlegen	Fügt ein Zeichen für das Textende ein und setzt den Cursor an die Ausgangsposition
Nt /	Lokal festlegen	

Tasten	Zuordnung	Beschreibung
		Setzt die Sitzung in den lokalen Modus
Nt *	Empfangen festlegen	Setzt die Sitzung in den Empfangsmodus
Eingabe	Eingabe	Sendet die Eingabetaste an den Host
Nt Eingabe	Eingabe	Sendet die Eingabetaste an den Host
Strg+A	Alles auswählen	Markiert den gesamten Text
Umschalt+Nach unten	Nach unten auswählen	Erweitert die Markierung von Text nach unten
Umschalt+Nach links	Nach links auswählen	Erweitert die Markierung von Text nach links
Umschalt+Nach rechts	Nach rechts auswählen Erweitert die Markierung von Text nach rechts	
Umschalt+Nach oben	Nach oben auswählen	Erweitert die Markierung von Text nach oben
Umschalt+Strg+1	Umschalt+F1	Sendet die Umschalt+F1-Taste an den Host
Umschalt+Strg+0	Umschalt+F10	Sendet die Umschalt+F10-Taste an den Host
Umschalt+Strg+2	Umschalt+F2	Sendet die Umschalt+F2-Taste an den Host
Umschalt+Strg+3	Umschalt+F3	Sendet die Umschalt+F3-Taste an den Host
Umschalt+Strg+4	Umschalt+F4	Sendet die Umschalt+F4-Taste an den Host
Umschalt+Strg+5	Umschalt+F5	Sendet die Umschalt+F5-Taste an den Host
Umschalt+Strg+6	Umschalt+F6	Sendet die Umschalt+F6-Taste an den Host

Tasten	Zuordnung	Beschreibung
Umschalt+Strg+7	Umschalt+F7	Sendet die Umschalt+F7-Taste an den Host
Umschalt+Strg+8	Umschalt+F8	Sendet die Umschalt+F8-Taste an den Host
Umschalt+Strg+9	Umschalt+F9	Sendet die Umschalt+F9-Taste an den Host
F5	Angeben	Überträgt die Cursorposition an den Host
Tab	Tabulator	Bewegt den Cursor in das nächste Feld
F2	Übertragen	Überträgt die Seite an den Host
Nt +	Übertragen	Überträgt die Seite an den Host
Strg+F2	Zeile übertragen	Überträgt die aktuelle Zeile an den Host
Nt -	Zeile übertragen	Überträgt die aktuelle Zeile an den Host

ALC-Tastaturbelegung

Tasten	Zuordnung	Beschreibung
Strg + M	Automatisch nach unten	Schaltet die Sitzungsfunktion zum Empfangen mehrerer Seiten ein bzw. aus.
Rücktaste	Rücktaste	Bewegt den Cursor um eine Spalte nach links
Umschalt+Tab	Rücktabulator	Bewegt den Cursor in das vorherige Feld
Strg+Pos1	Löschen	Entfernt den Bildschirminhalt und sendet die Löschtaste an den Host
Strg+B	Broadcast löschen	Löscht die SITA-Broadcast-Meldung.
:	Doppelpunkt	Fügt ein Doppelpunktzeichen an der Cursorposition ein
Strg+L	Lothringer Kreuz	Fügt das Lothringer Kreuz-Zeichen an der Cursorposition ein.
↓	Cursor nach unten	Bewegt den Cursor um eine Zeile nach unten.
Nt ↓	Cursor nach unten	Bewegt den Cursor um eine Zeile nach unten.
←	Cursor nach links	Bewegt den Cursor zum vorherigen Wort
Nt ←	Cursor nach links	Bewegt den Cursor zum vorherigen Wort
→	Cursor nach rechts	Bewegt den Cursor zum nächsten Wort
Nt →	Cursor nach rechts	Bewegt den Cursor zum nächsten Wort
↑	Cursor nach oben	Bewegt den Cursor um eine Zeile nach oben.
Nt ↑	Cursor nach oben	Bewegt den Cursor um eine Zeile nach oben.
Löschen	Zeichen löschen	Löscht das Zeichen an der Cursorposition
Strg+Entf	Zeile löschen	Löscht die Zeile an der Cursorposition

Tasten	Zuordnung	Beschreibung
=	Anzeige	Fügt das Anzeigezeichen an der Cursorposition ein
Strg + N	Neue Zeile anzeigen	Fügt das Anzeigezeichen in einer neuen Zeile ein.
]	Dollar	Fügt das US-Dollarzeichen an der Cursorposition ein.
.	Elementende	Fügt das Zeichen für das Endelement an der Cursorposition ein.
Ende	Zeilenende	Bewegt den Cursor an das Zeilenende.
Strg+T	Transaktionsende	Schließt den PNR.
Strg+E	Anzeigeende löschen	Löscht alle Daten ab der Cursorposition bis zum Ende der Anzeige.
Strg+Ende	Zeilenende löschen	Löscht alle Daten ab der Cursorposition bis zum Ende der Zeile.
Pos1	Pos1	Bewegt den Cursor in das erste ungeschützte Feld auf dem Bildschirm
Strg+I	Ignorieren	Verwirft alle am aktuellen PNR vorgenommenen Änderungen.
Strg+Einfg	Zeile einfügen	Einfügen einer neuen Zeile im Bildschirmspeicher
Einf	Einfügen Leerzeichen	Fügt ein neues Leerzeichen in den Bildschirmspeicher ein.
\	Neue Zeile	Fügt das Neue-Zeile-Zeichen an der Cursorposition ein.
[	Allgemeines Währungssymbol	Fügt das allgemeine Währungssymbol an der Cursorposition ein.
Strg+G	Pfund	Fügt ein britisches Pfund-Zeichen an der Cursorposition ein.
Strg+Eingabetaste	Print Enter	Sendet die Antwort an den Drucker.
Strg+P	Geschützter Reset	Bewegt den Cursor in das erste ungeschützte Feld.

Tasten	Zuordnung	Beschreibung
Strg+↑	Nächste Eingabe aufrufen	Ruft die nächste Eingabe auf.
Strg+↓	Vorherige Eingabe aufrufen	Ruft die vorherige Eingabe auf.
Strg + Z	Erneut eingeben	Sendet die zuvor gesendete Meldung erneut an den Host.
Strg+R	Wiederholen	Zeigt die letzte vom Host gesendete Meldung erneut an.
Esc	Zurücksetzen	Setzt Tastaturfehler zurück
Umschalt+Strg+↓	Zeile nach unten blättern	Blättert die Anzeige eine Zeile nach unten.
Umschalt+Strg+↑	Zeile nach oben blättern	Blättert die Anzeige eine Zeile nach oben.
Bild nach unten	Seite nach unten blättern	Blättert die Anzeige eine Seite nach unten.
Bild nach oben	Seite nach oben blättern	Blättert die Anzeige eine Seite nach oben.
Strg+A	Alles auswählen	Markiert den gesamten Text
Umschalt+↓	Nach unten auswählen	Erweitert die Markierung des gesamten Texts nach unten.
Umschalt+↑	Nach oben auswählen	Erweitert die Markierung des gesamten Texts nach oben.
Umschalt+←	Nach links auswählen	Erweitert die Markierung des gesamten Texts nach links.
Umschalt+→	Nach rechts auswählen	Erweitert die Markierung des gesamten Texts nach rechts.
‘	Start der Meldung	Fügt ein Beginn-der-Meldung-Zeichen an der Cursorposition ein.
F12	Statistik	Zeigt die Kommunikationsstatistik an.
Tab	Tabulator	Bewegt den Cursor in das nächste ungeschützte Feld

Tasten	Zuordnung	Beschreibung
Strg + F	CODACOM ein-/ ausschalten	Schaltet den CODACOM-Modus ein/aus.
Eingabe	Übertragen	Übermittelt die Seite an den Host.
Nt Eingabe	Übertragen	Übermittelt die Seite an den Host.
Umschalt+Eingabe	Übertragen	Übermittelt die Seite an den Host.
Umschalt+Esc	Tastatursperre aufheben	Hebt die Tastatursperre auf.
Strg+U	Nicht angeforderte Meldung	Ruft eine nicht angeforderte Meldung vom Host ab.

5.4 Dateiübertragung

Host Access for the Cloud unterstützt drei verschiedene Dateiübertragungsprotokolle:

- IND$FILE für 3270-Host-Übertragungen
- AS/400 für 5250-Host-Übertragungen
- File Transfer Protocol (FTP), mit dem ein lokaler Computer als FTP-Client fungieren kann.

Sobald die Verbindung hergestellt ist, können Sie auf dem Server Dateien anzeigen und mithilfe von FTP Dateien zwischen dem lokalen Computer (bzw. einem beliebigen Netzlaufwerk) und dem FTP-Server übertragen.

Für FTP-Übertragungen ist die Batchdateiübertragung verfügbar. Mit dieser Option können Sie mehrere Dateien in einem Vorgang herunterladen und hochladen.

Bevor Sie Dateien übertragen oder senden können, muss der Administrator die Übertragungs- und Sendeoptionen für die aktuelle Sitzung aktivieren und die erforderlichen Konfigurationseinstellungen vornehmen. Dies erfolgt im Bereich „Dateiübertragungseinstellungen“.

Abhängig von dem zu verwendenden Hostdateisystem und der zu verwendenden Übertragungsart werden unterschiedliche Konfigurationsoptionen angezeigt. Nach der Konfiguration ist das Dialogfeld „Dateiübertragung“ in der Symbolleiste verfügbar.

- IND$FILE
- AS/400
- FTP
- Batchübertragungen

5.4.1 IND$FILE

IND$FILE ist ein Dateiübertragungsprogramm von IBM, mit dem Sie Informationen zwischen Ihrem Computer und einem 3270-Hostcomputer übertragen können.

Wählen Sie in der Dropdown-Liste „Hostdateisystem“ aus, welche IBM 3270-Betriebsumgebung auf dem Host ausgeführt wird. Host Access for the Cloud unterstützt TSO (Time Sharing Option), CMS (Conversational Monitor System) und CICS. Die Standardeinstellung ist „Keine“.

Es werden Übertragungen im ASCII- oder Binär-Modus unterstützt. Wenn eine Verbindung mit einem TSO-Host besteht, können Sie zudem direkt zu einem bestimmten TSO-Datensatz navigieren.

Allgemeine Optionen für CICS-, CMS- und TSO-Hostdateitypen

Hostdateien automatisch anzeigen – Die Hostdateiliste enthält standardmäßig alle Hostdateien, die zur Übertragung verfügbar sind. Deaktivieren Sie diese Option, um Hostdateien nur abzurufen,

wenn Sie sie anfordern. Klicken Sie im Dialogfeld „Übertragen“ auf „Hostdateien anzeigen“, um die Hostdateien abzurufen.

Übertragungsoptionen für CICS-, CMS- und TSO-Hostdateitypen

Option	Beschreibung
Übertragungsart	• Binär – Für Programmdateien und andere Dateitypen, die nicht konvertiert werden sollten. Dies gilt beispielsweise für Dateien mit anwendungsspezifischer Formatierung oder für Dateien, die bereits für einen bestimmten Druckertyp formatiert wurden. Binärdateien enthalten nicht druckbare Zeichen. Wenn Sie diese Übertragungsart wählen, werden die Dateien während der Übertragung nicht konvertiert (umgewandelt). • ASCII – Zur Übertragung von Textdateien ohne besondere Formatierung. ASCII-Dateien auf dem PC werden in den EBCDIC-Zeichensatz auf dem Host übersetzt und Hosttextdateien werden beim Herunterladen von EBCDIC in ASCII konvertiert.
CR/LF-Verarbeitung	Wenn diese Option ausgewählt ist, werden Wagenrücklauf/Zeilenvorschub-Paare von an den Host gesendeten Dateien entfernt und am Ende jeder Zeile in vom Host empfangenen Dateien hinzugefügt.
Hoststartbefehl	Gibt das Hostprogramm an, mit dem die Dateiübertragung initiiert wird. Die Standardeinstellung „IND$FILE“ ist für CMS- und TSO-Hosts geeignet. Für CICS-Hosts ist „IND$FILE“ unter Umständen ebenfalls geeignet; andernfalls müssen Sie die CICS-Transaktion Ihres Hosts angeben (z. B. CFTR).
Startparameter	Verwenden Sie dieses Feld für alle Parameter auf Ihrem Hostsystem, die zum IND$FILE-Programm gehören. Der Inhalt dieses Felds wird an das Ende des Übertragungsbefehls angefügt, der in Host Access for the Cloud generiert wird. Host Access for the Cloud bestätigt die Parameter nicht.
Max. Feldgröße	Wählen Sie eine Feldgröße für das WSF-Protokoll aus. Der Standardwert lautet 4 Kilobyte. Normalerweise gilt, dass die Übertragung mit zunehmender Puffergröße schneller erfolgt. Die meisten Systeme unterstützen 8 KB. Wenn Sie einen für den Host zu hohen Wert auswählen, wird die Sitzung beim ersten Übertragen einer Datei, die den gesamten Puffer belegt, automatisch getrennt. Im Allgemeinen gibt die Person, die die Software für die Hostkommunikation installiert, diesen Wert an. Das Host-TCP/IP-Produkt von IBM bezieht diesen Wert beispielsweise aus dem Parameter DATABUFFERPOOLSIZE, dessen Standardwert auf 8-KB-Puffer eingestellt wird. Wenn Sie nicht wissen, welchen Wert Sie hier eingeben sollen, wenden Sie sich an Ihren Systemadministrator.
Erstschlüssel	

	Sie können vor der Übertragung oder Auflistung von Dateien bestimmte Aktionen festlegen. Sie können „Keine“, „Autom. Erkennung“ oder „Löschen“ auswählen. Wenn „Keine“ ausgewählt wurde, dann wird LISTCAT automatisch ausgestellt. Wenn „Autom. Erkennung“ ausgewählt ist, werden die aktuellen Bildschirminhalte überprüft, um zu bestimmen, ob ein LISTCAT oder TSO LISTCAT versendet werden soll. Wenn „Löschen“ ausgewählt ist, wird vor der Ausgabe des Befehls die Löschtaste gesendet. Für TSO bedeutet Löschen auch, dass „TSO“ nicht dem Dateianforderungsbefehl vorangestellt wird.
PC-Codeseite	Der zum Lesen oder Schreiben lokaler Dateien während einer Dateiübertragung zu verwendende Zeichensatz. Der Wert **Standard** verwendet die Codeseite, die dem Gebietsschema Ihres Betriebssystems entspricht. Wenn Sie für die Angabe der PC-Codeseite einen anderen Zeichensatz benötigen, wählen Sie ihn in der Liste aus.
Hostcodeseite	Der beim Umwandeln von EBCDIC-Zeichen während der Übertragung von Dateien zum oder vom Host zu verwendende Zeichensatz. Der Standardwert **NCS-Einstellung verwenden** verwendet den im Bereich „Anzeige“ unter „Terminal“ angegebenen nationalen Zeichensatz. Wenn Sie für die Angabe der Host-Codeseite einen anderen Zeichensatz benötigen, wählen Sie ihn in der Liste aus.
Antwortzeitlimit (Sekunden)	Legt fest, wie viele Sekunden auf eine Hostantwort gewartet werden soll, bevor Host Access for the Cloud abbricht und eine Fehlermeldung zurückgibt. Der Standardwert ist 60 Sekunden.
Startzeitlimit (Sekunden)	Legt die Dauer in Sekunden fest, während der Host Access for the Cloud beim Verbindungsaufbau zum Host auf eine Hostantwort warten soll. Wenn die angegebene Zeit ohne eine Hostantwort verstrichen ist, bricht Host Access for the Cloud infolge Zeitüberschreitung ab und gibt eine Fehlermeldung zurück. Der Standardwert ist 25 Sekunden.

Sendeoptionen für CICS-, CMS- und TSO-Hostdateitypen

Option	Beschreibung	Gilt für diesen Hosttyp
Datensatzformat	Mit dieser Option geben Sie das Datensatzformat für an den Host gesendete Dateien an. • Standard – Der Host bestimmt das Datensatzformat. Dies ist die Standardoption. • Fest – Zwingt den Host, Datensätze mit einer bestimmten Länge zu erstellen. • Nicht definiert – Zwingt den Host, Dateien ohne ein bestimmtes Datensatzformat zu erstellen (dieser Wert ist nur für TSO-Systeme relevant). • Variabel – Zwingt den Host, Datensätze mit einer variablen Länge zu erstellen, wobei das Binärdateiformat erhalten bleibt.	TSO, CMS
Zuordnungseinheiten	Gibt die Festplattenunterteilungen für Ihre primäre und sekundäre Speicherzuweisung an. Wenn Sie Standard auswählen (Standardwert), wird die Einheit vom Host festgelegt. Sie können auch die Optionen Zylinder, Spur oder Block wählen. Wenn Sie Block wählen, geben Sie im Feld Durchschnittsblock die durchschnittliche Blockgröße (in Byte) an.	TSO
Logische Datensatzlänge	Die Datensatzgröße (in Byte) für die auf dem Host zu erstellende Datei. Wenn Sie dieses Feld leer lassen, wird die Datensatzgröße vom Host bestimmt. Zwischen 0 und 32767 können Sie einen Wert in dem von Ihrem Host akzeptierten Bereich festlegen. Diese Option ist für CICS-Hosts nicht verfügbar. Stellen Sie bei ASCII-Dateien diesen Wert so ein, dass die längste Zeile in Ihrer Datei hineinpasst. Wenn Sie das Feld frei lassen, akzeptiert der Host normalerweise Zeilen von bis zu 80 Zeichen.	TSO, CMS
Wenn Hostdatei vorhanden		TSO, CMS

	Gibt an, wie bei der Übertragung vorgegangen wird, wenn eine Datei mit dem gleichen Namen bereits vorhanden ist. • Anfügen – Fügt den Inhalt der lokalen Datei an die vorhandene Hostdatei an. • Überschreiben – Überschreibt den Inhalt der Hostdatei. Bei CICS-Systemen kann nicht ermittelt werden, ob eine solche Hostdatei bereits existiert. Somit ist die Option Überschreiben die einzige Möglichkeit für das Senden von Dateien an ein CICS-System.	
Blockgröße (Byte)	Gibt bei TSO-Hosts die Blockgröße für die auf dem Host zu erstellende Datei an. Für Dateien mit Datensätzen fester Länge muss dieser Wert ein Vielfaches des Werts im Feld „Logische Datensatzlänge“ darstellen (weil Blöcke in logische Datensätze unterteilt sind). Sie können einen beliebigen Wert zwischen 0 und 32767 festlegen, um einen beliebigen vom Host akzeptierten Bereich zu berücksichtigen.	TSO
Durchschnittsblock (Byte)	Die Größe für einen Durchschnittsblock. Dieser Wert ist nur relevant, wenn Sie Blöcke als Zuordnungseinheit verwenden.	TSO
Primäre Zuordnung (Zuordnungseinheiten)	Die Größe der primären Zuordnung für die zu erstellende Hostdatei.	TSO
Sekundäre Zuordnung (Zuordnungseinheiten)	Die Größe zusätzlicher Zuordnungen für den Fall, dass die primäre Zuordnung nicht ausreicht. Mehrfache sekundäre Speicherplatzzuordnungen sind bis zu einer vom Host festgelegten Grenze zulässig (in der Regel 15).	TSO

Hinweis

Wenn Sie CICS als Hostsystem verwenden, müssen Sie die Namen der Dateien, die Sie übertragen, manuell eingeben. In diesem Fall ist keine Liste zum Auswählen der Dateien verfügbar.

Dateien übertragen (IND$FILE)

Sie müssen mit dem Host verbunden und bei diesem angemeldet sein, um Dateien für die aktuelle 3270-Sitzung übertragen zu können.

1. Stellen Sie sicher, dass sich der Host in einem betriebsbereiten Status befindet, um den IND$FILE-Befehl akzeptieren zu können.
2. Klicken Sie in der Symbolleiste auf das IND$FILE-Symbol  .
3. Das Dialogfeld „Dateiübertragung“ zeigt eine Liste der Hostdateien und -verzeichnisse, die zur Übertragung verfügbar sind. Verzeichnisse und Dateien werden bei der Auswahl der Datei durch ein entsprechendes Symbol gekennzeichnet. Geben Sie für CICS-Hosts die Namen der zu übertragenden Dateien ein.
4. Wählen Sie die Übertragungsmethode aus: Die Optionen sind:

   - Binär

     Für Programmdateien und andere Dateitypen, die nicht konvertiert werden sollen. Dies gilt beispielsweise für Dateien mit anwendungsspezifischer Formatierung oder für Dateien, die bereits für einen bestimmten Druckertyp formatiert wurden. Binärdateien enthalten nicht druckbare Zeichen. Wenn Sie diese Übertragungsart wählen, werden die Dateien während der Übertragung nicht konvertiert (umgewandelt).

   - ASCII

     Zur Übertragung von Textdateien ohne besondere Formatierung. ASCII-Dateien auf dem PC werden in den EBCDIC-Zeichensatz auf dem Host übersetzt, und Hosttextdateien werden beim Herunterladen von EBCDIC in ASCII konvertiert.

5. Wenn eine Verbindung mit einem TSO-Host hergestellt ist, klicken Sie auf „Ebene“, um den neuen anzuzeigenden Datensatz einzugeben. Host Access for the Cloud aktualisiert die Remotedateiliste mit der angegebenen Datensatzebene.

> **Hinweis**
>
> Bei Angabe von Dateien mit *Hochladen als* oder *Herunterladen* muss ein vollständiger Datengruppenname in einfache Anführungszeichen gesetzt werden. Datengruppennamen, die nicht in einfache Anführungszeichen gesetzt werden, wird standardmäßig ein in TSO PROFILE angegebener allgemeiner Qualifizierer vorangestellt.

Sie können die Dateiliste jederzeit aktualisieren, indem Sie im Dialogfeld „Dateiübertragung“ links oben auf das Symbol „Aktualisieren“ klicken.

- Dateien herunterladen (IND$FILE)
- Dateien hochladen (IND$FILE)
- Fehlerbehebung für Dateiübertragungen

Dateien herunterladen (IND$FILE)

1. Klicken Sie in der Liste auf den Namen der Datei, um die Übertragung zu initiieren.

   oder

   Klicken Sie auf **Herunterladen**, und geben Sie den Namen der zu übertragenden Hostdatei ein. Sie können Dateien von TSO- sowie CMS-Hosttypen herunterladen. In TSO und CMS werden Hostdateien allerdings unterschiedlich dargestellt, d. h., Sie müssen den Dateinamen in der Eingabeaufforderung jeweils in einem unterschiedlichen Format eingeben.

   - **TSO**: Setzen Sie den Namen des Hostpfads in einfache Anführungszeichen, um den vollständigen Datensatznamen anzugeben. Beispiel: `'BVTST03.DATA.TXT'`. Um einen Dateispeicherort anzugeben, der relativ zur zuvor angegebenen Datensatzebene ist, verwenden Sie keine einfachen Anführungszeichen. `DATA.TXT` gibt beispielsweise den gleichen Datensatz an, jedoch relativ zu `BVTST03`.
   - **CMS**: Eine typische CMS-Eingabe ist beispielsweise `BVTSTT01 DATA A1`. Die Verwendung einfacher Anführungszeichen ist nicht erforderlich.

2. Falls nötig, können Sie die Übertragung im Bereich mit dem Fortschritt der Übertragung abbrechen.

Dateien hochladen (IND$FILE)

> **Hinweis**
>
> IBM-Mainframe-Computersysteme schreiben bestimmte Namenskonventionen für Dateien vor. Detaillierte Informationen zu den Anforderungen bei der Namensgebung finden Sie in der IBM-Dokumentation.

Wählen Sie eine der beiden Methoden zum Hochladen von Dateien aus:

- Klicken Sie im Dialogfeld **Dateiübertragung** auf **Hochladen**.

  Sie können einen anderen Namen für die hochgeladene Datei angeben. Klicken Sie auf „Hochladen als“, navigieren Sie zu der hochzuladenden Datei und geben Sie bei der entsprechenden Aufforderung den Namen ein, den Sie verwenden möchten. Denken Sie daran, dass bei hergestellter Verbindung mit einem TSO-Host ein vollständiger Datengruppenname in einfache Anführungszeichen gesetzt werden muss. Siehe Schritt 5 unter „Dateien übertragen“.

  Alternativ:

- Ziehen Sie die hochzuladende Datei von ihrem Speicherort in das Dialogfeld **Dateiübertragung**. Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass die Datei erfolgreich hochgeladen wurde.

Wenn Sie den Hochladeprozess abbrechen, bevor eine Datei vollständig übertragen wurde, verbleibt eine unvollständige Datei auf dem Host.

Fehlerbehebung für Dateiübertragungen

In einigen Fällen kann es bei einer Dateiübertragung zu Fehlern kommen. Diese Fehler können Mainframe-Probleme sein oder durch Sicherheitseinstellungen des Browsers verursacht werden.

- Wenn eine Übertragung erfolgt ist, die Datei jedoch nicht die erwarteten Daten enthält, überprüfen Sie, ob die Übertragungsart korrekt auf „Binär“ oder „ASCII“ festgelegt ist.
- Für Dateiübertragungen gilt beim Hochladen ein Dateigrößenlimit von 50 MB. Sie können diesen Wert ändern.
- Informationen zu hostspezifischen Fehlern finden Sie unter IBM File Transfer Error Messages (IBM-Fehlermeldungen bei der Dateiübertragung)

5.4.2 AS/400

Mit der AS/400-Dateiübertragung können Sie Daten zwischen Ihrem Computer und einem iSeries-Host übertragen.

AS/400-Dateiübertragungen sind im Allgemeinen einfach und unkompliziert. Da die Hostdaten als DB2-Datenbank verwaltet werden, können Sie jedoch mit SQL Editor recht komplexe Abfragen erstellen.

So konfigurieren Sie die AS/400-Dateiübertragung

1. Erstellen Sie eine HACloud-5250-Terminalsitzung, geben Sie einen Hostnamen oder eine Hostadresse ein und legen Sie einen Namen für die Sitzung fest.
2. Wählen Sie im Einstellungsbereich die Option „Dateiübertragung“.
3. Wählen Sie „AS/400 aktivieren“ aus und fahren Sie mit der Konfiguration fort.

    - **Host**

      Das Hostfeld wird mit der für die Terminalsitzung angegebenen Hostadresse ausgefüllt. Bei Bedarf können Sie einen anderen Host angeben. Um einen anderen Port anzugeben, fügen Sie die Portnummer an die Hostadresse an. Beispiel: host.meinefirma.com:23.

    - **TLS-Sicherheit**

      Wählen Sie in der Dropdown-Liste die gewünschte TLS-Sicherheitsoption aus.

      Bei Verwendung dieser Option: Das Zertifikat des AS/400-Datenbankservers muss in MSS zur Liste der verbürgten Zertifikate hinzugefügt werden. Wenn das Zertifikat noch nicht hinzugefügt wurde, befolgen Sie die Anweisungen unter Trusted Certificates (Verbürgte Zertifikate) in der MSS-Dokumentation.

    - **Standardmäßige Übertragungsmethode**

      Legen Sie die bevorzugte standardmäßige Übertragungsmethode fest: Text mit fester Breite oder durch Kommas getrennte Werte (CSV, Comma Separated Values). Die Übertragungsmethode kann beim Ausführen einer Übertragung geändert werden.

    - **Spaltenüberschriften standardmäßig einschließen**

      Aktivieren Sie diese Option, um für alle heruntergeladenen Daten standardmäßig Spaltenüberschriften einzuschließen. Sie können diese Einstellung für jedes Herunterladen im Dialogfeld der Dateiübertragung ändern.

      Die Spaltenüberschriften stammen nicht aus der Hostdatei, sondern werden beim Herunterladen einer Datei hinzugefügt. Sie werden automatisch entfernt, wenn eine Datei hochgeladen wird.

4. Klicken Sie auf **Speichern** und stellen Sie eine Verbindung zur Sitzung her.

Dateien übertragen (AS/400)

Nachdem die Sitzung zur Verwendung der AS/400-Dateiübertragung konfiguriert wurde, klicken Sie in der Symbolleiste auf  , um das Dialogfeld **Dateiübertragung** zu öffnen. Das Dialogfeld

enthält eine Liste der Hostdateien, die zur Übertragung verfügbar sind. Wenn Sie dazu aufgefordert werden, geben Sie Ihre AS/400-Anmeldeberechtigung ein.

- Dateien herunterladen (AS/400)
- Mit SQL herunterladen
- Dateien hochladen (AS/400)
- Bibliothek hinzufügen

DATEIEN HERUNTERLADEN (AS/400)

Das AS/400-Dateisystem umfasst Bibliotheken, Dateien und Mitglieder. Bibliotheken werden durch dieses Symbol identifiziert: . Sie können Bibliotheken nicht herunterladen, aber auf eine Bibliothek klicken, um die darin enthaltenen Dateien und Mitglieder anzuzeigen.

Wählen Sie **Spaltenüberschriften einschließen** aus, um die Spaltenüberschriften für heruntergeladene Daten anzuzeigen.

1. Öffnen Sie die Bibliothek, in der die Dateien enthalten sind ( ).
2. Erweitern Sie die Datei, in der das Mitglied enthalten ist, das Sie herunterladen möchten.
3. Klicken Sie auf ein Mitglied, um es herunterzuladen.
4. Öffnen Sie den Download-Ordner des Browsers, um sich zu vergewissern, dass die Datei dort vorhanden ist. Öffnen Sie die Datei in einem Texteditor.

HERUNTERLADEN MIT SQL

Sie können SQL-Abfragen erstellen, um nur die Daten abzurufen, die Sie von einem Dateimitglied auf dem Host benötigen. Auf diese Weise können Sie bestimmte Felder auswählen und andere ignorieren.

1. Öffnen Sie die Bibliothek und die Datei, die Sie herunterladen möchten.
2. Öffnen Sie das Optionsmenü und klicken Sie auf **SQL**.

3. SQL Editor wird geöffnet und enthält die SELECT-Anweisung, mit der das gesamte Mitglied heruntergeladen wird. Das Dateimitglied wird als BIBLIOTHEKSNAME/DATEINAME(MITGLIEDSNAME) referenziert.
4. Klicken Sie auf **Ausführen**, um das gesamte Mitglied herunterzuladen oder bearbeiten Sie die SQL-Anweisung und klicken Sie dann auf „Ausführen“, um einen Teilsatz der Daten abzurufen.

DATEIEN HOCHLADEN (AS400)

Sie können Daten nur als neue Mitglieder oder Ersatzmitglieder in Dateien hochladen. Die AS/400-Datei enthält eine Spezifikation zur Beschreibung der Daten in den Mitgliedern und jedes Mitglied in einer bestimmten Datei weist die gleiche Struktur auf. Typischerweise ist es nicht möglich (bzw. nicht empfehlenswert), ein Mitglied aus einer Datei herunterzuladen und in eine andere Datei hochzuladen, sofern nicht beide Dateien die gleiche Datenspezifikation haben.

Da die Daten nur als Mitglieder hochgeladen werden können, müssen Sie eine Datei öffnen und ihre Mitglieder im Dialogfeld der Dateilisten anzeigen, bevor die Schaltfläche „Hochladen“ aktiviert wird.

1. Öffnen Sie die Datei, in die Sie Mitglieder hochladen möchten. Die Schaltfläche „Hochladen“ ist nun verfügbar.
2. Führen Sie eine der beiden folgenden Aktionen aus:

   Klicken Sie auf die Schaltfläche **Hochladen** und wählen Sie eine Datei zum Hochladen aus dem lokalen Dateisystem aus.

   Alternativ:

   Klicken Sie auf den Abwärtspfeil der Schaltfläche „Hochladen“ und wählen Sie **Hochladen als...** aus. Wählen Sie dann die Datei aus, legen Sie einen neuen Namen für die Datei fest und klicken Sie auf „OK“.

BIBLIOTHEK HINZUFÜGEN

Als AS/400-Benutzer haben Sie typischerweise Zugriff auf einen bestimmten Satz an Bibliotheken, der von einem Systemadministrator zugewiesen wurde. Diese Bibliotheken werden im Dialogfeld der Dateiübertragung als Einträge der obersten Ebene angezeigt. Wenn Sie Zugriff auf eine Bibliothek benötigen, die nicht in der Liste enthalten ist, kann der Systemadministrator die Konfiguration so aktualisieren, dass die neue Bibliothek zu Ihrer Liste hinzugefügt wird. Wenn Sie nur vorübergehend mit einer bestimmten Bibliothek arbeiten müssen, ist es nicht erforderlich, diese Bibliothek dauerhaft zu Ihrer Bibliotheksliste hinzufügen zu lassen.

So fügen Sie eine Bibliothek hinzu

Öffnen Sie das Dialogfeld für die AS/400-Dateiübertragung und klicken Sie auf **Bibliothek hinzufügen**. Diese Schaltfläche ist im Bereich der Bibliotheksliste verfügbar. Diese Hinzufügung ist nicht dauerhaft und Sie müssen die Bibliothek erneut hinzufügen, wenn Sie das Dialogfeld der Dateiübertragung schließen und erneut öffnen.

5.4.3 FTP

Mit Host Access for the Cloud können Sie einen lokalen Computer als FTP-Client verwenden. Mit diesem FTP-Client können Sie Verbindungen zu einem FTP-Server herstellen, der auf einem anderen Computer ausgeführt wird. Sobald die Verbindung hergestellt ist, können Sie auf dem Server Dateien anzeigen und mithilfe von FTP Dateien zwischen dem lokalen Computer (bzw. einem beliebigen Netzlaufwerk) und dem FTP-Server übertragen. Über FTP kann ein Client Dateien

auf einem Server hochladen, herunterladen, löschen, umbenennen, verschieben und kopieren, entweder einzeln oder als Batchübertragung, bei der Sie eine Liste der Dateien erstellen können, die in einem Vorgang übertragen werden.

> **Tipp**
>
> Wenn Sie eine Batchübertragung planen, wählen Sie zuerst die Option „FTP aktivieren“ aus und konfigurieren Sie die Option.

So konfigurieren Sie FTP

Wählen Sie „FTP aktivieren“ aus und fahren Sie mit der Konfiguration fort:

- **Protokoll**

  Verwenden Sie FTP, um eine FTP-Standardsitzung zu starten. Verwenden Sie SFTP, um eine SFTP-Sitzung zu starten.

  Sie können einen FTP-Client zur Verwendung des SFTP-Protokolls einrichten und alle Operationen über einen verschlüsselten Secure Shell-Transport durchführen. Host Access for the Cloud verwendet einen Benutzernamen und ein Passwort zur Authentifizierung.

- **Host**

  Geben Sie den Hostnamen oder die IP-Adresse des FTP-Servers an, mit dem Sie eine Verbindung herstellen möchten.

- **Port**

  Der Port des angegebenen FTP-Servers.

- **Wenn beim Dateiupload Remotedatei vorhanden**

  Geben Sie an, wie die Übertragung erfolgen soll, wenn bereits eine Datei mit dem gleichen Namen vorhanden ist.

Option	Beschreibung
Anfügen	Die gesendete Datei wird an die vorhandene Datei angefügtB1
Benutzer fragen (Standard)	Es wird gefragt, wie mit dem doppelten Dateinamen umgegangen werden soll.
Abbrechen	Die Dateiübertragung wird abgebrochen.
Fehler	Die Dateiübertragung wird abgebrochen, und Sie erhalten eine Fehlerbenachrichtigung.
Überschreiben	Die auf dem Remotecomputer bereits vorhandene Datei wird überschrieben.
Überspringen	Wenn eine Anforderung mehrere Dateien umfasst, wird die Datei, deren Name mit einem vorhandenen Dateinamen übereinstimmt übersprungen, die Übertragung der anderen Dateien wird jedoch fortgesetzt.
Eindeutig	Eine neue Datei mit einem eindeutigen Dateinamen wird erstellt.

- **Ursprüngliches Remoteverzeichnis**

  Geben Sie den Pfad zu einem Ausgangs- oder Standardverzeichnis der FTP-Site an. Nachdem die Verbindung zum FTP-Server hergestellt ist, wird dort automatisch das angegebene Standardverzeichnis als Arbeitsverzeichnis aktiviert. Die Dateien und Ordner im Standardverzeichnis des Servers werden im FTP-Sitzungsfenster angezeigt. Wenn das anfängliche Remoteverzeichnis nicht gefunden wird, wird eine Warnmeldung angezeigt und die Verbindung bleibt bestehen.

- **Anonymer Benutzer**

  Wählen Sie diese Option aus, wenn Sie sich bei dem angegebenen FTP-Server als Gast mit dem Benutzernamen „anonymous“ anmelden möchten. Wenn auf dem Host, mit dem die Verbindung hergestellt wird, anonyme Benutzer nicht unterstützt werden, müssen Sie möglicherweise Ihre Anmeldeinformationen angeben.

- **Sitzungstimeout (Sekunden)**

  Anhand dieses Werts erkennt der FTP-Client, wie viele Sekunden er auf die Übertragung von Datenpaketen vom bzw. zum Host warten soll. Wenn innerhalb des angegebenen Zeitraums keine Daten eingehen, werden Sie über eine Fehlermeldung darauf hingewiesen, dass die Wartezeit abgelaufen ist, und die Übertragung wird abgebrochen. Wiederholen Sie in diesem Fall den Vorgang. Wenn auch bei wiederholten Versuchen immer wieder Fehlermeldungen angezeigt werden, erhöhen Sie die Wartezeit. Wenn in diesem Feld der Wert 0 (Null) eingegeben ist, tritt auf dem SFTP-Client beim Warten auf eine Antwort überhaupt keine Zeitüberschreitung ein. Für SFTP-Sitzungen lautet der Standardwert 0 (Null).

- **Keep Alive-Zeit (Sekunden)**

  Wählen Sie diese Option aus, und geben Sie einen entsprechenden Sekundenwert ein, wenn Ihre Serververbindung über die am Server eingestellte automatische Wartezeit bei Inaktivität hinaus aufrechterhalten werden soll. Die meisten Server verfügen über einen Leerlaufzeitwert, mit dem angegeben wird, wie lange die FTP-Sitzung eines Benutzers bei festgestellter Inaktivität fortgesetzt wird. Überschreitet der Benutzer diese Zeitbeschränkung, wird die Server-Verbindung beendet.

  Mit dieser Einstellung wird der FTP-Client angewiesen, in festgelegten Intervallen einen NOOP-Befehl an den Server zu senden, damit der Server die Verbindung nicht aufgrund von Inaktivität trennt. Bedenken Sie aber, dass Sie durch die so erzwungene Fortsetzung Ihrer Sitzung unter Umständen andere Benutzer daran hindern, eine Verbindung zum FTP-Server herzustellen.

- **Hostcodierung**

  Definiert den Zeichensatz, den der Host für die Anzeige der Namen von übertragenen Dateien verwendet. Standardmäßig verwendet Host Access for the Cloud UTF-8 (Unicode). Wenn Sie Dateien mit der Standardeinstellung übertragen, aber die Dateinamen nicht gelesen werden können, ändern Sie die Hostcodierung in den vom Host verwendeten Zeichensatz. (Diese Option hat keinen Einfluss auf die Codierung von Dateiinhalten, sondern nur auf die Namen von Dateien.)

Dateien übertragen (FTP)

Nachdem der Administrator eine Sitzung für die FTP-Funktionalität konfiguriert hat, klicken Sie in der Symbolleiste auf  , um das Fenster für die FTP-Dateiübertragung zu öffnen, das eine

Liste mit Hostdateien enthält, die zur Übertragung verfügbar sind. Verzeichnisse und Dateien werden bei der Auswahl der Datei durch ein entsprechendes Symbol gekennzeichnet.

1. Wählen Sie die Übertragungsmethode aus: Die Optionen sind:

   - Binär

     Für Programmdateien und andere Dateitypen, die nicht konvertiert werden sollen. Dies gilt beispielsweise für Dateien mit anwendungsspezifischer Formatierung oder für Dateien, die bereits für einen bestimmten Druckertyp formatiert wurden. Binärdateien enthalten nicht druckbare Zeichen. Wenn Sie diese Übertragungsart wählen, werden die Dateien während der Übertragung nicht konvertiert (umgewandelt).

   - ASCII

     Zur Übertragung von Textdateien ohne besondere Formatierung. ASCII-Dateien auf dem PC werden in den EBCDIC-Zeichensatz auf dem Host übersetzt, und Hosttextdateien werden beim Herunterladen von EBCDIC in ASCII konvertiert.

2. Sie können eine Datei aus der Dateiliste umbenennen, löschen oder herunterladen.

3. Sie können die Dateiliste jederzeit aktualisieren, indem Sie im Dialogfeld „Dateiübertragung“ links oben auf das Symbol „Aktualisieren“ klicken.

Dateien herunterladen (FTP)

1. Wählen Sie in der Liste die Datei aus, um die Übertragung zu starten.
2. Falls nötig, können Sie die Übertragung im Bereich mit dem Fortschritt der Übertragung abbrechen.

Dateien hochladen (FTP)

Wählen Sie eine der beiden Methoden zum Hochladen von Dateien aus:

- Klicken Sie im Dialogfeld **Dateiübertragung** auf **Hochladen**.

  Wählen Sie im Fenster „Durchsuchen“ die hochzuladende Datei.

  Alternativ:

- Ziehen Sie die hochzuladende Datei von ihrem Speicherort in das Dialogfeld **Dateiübertragung**.

  Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass die Datei erfolgreich hochgeladen wurde.

Klicken Sie auf **Neues Verzeichnis**, um ein neues Verzeichnis auf dem Remoteserver zu erstellen. Sie werden aufgefordert, den Namen des neuen Verzeichnisses einzugeben.

5.4.4 Batchübertragungen

> **Hinweis**
>
> Damit Sie Batchübertragungen konfigurieren können, müssen Sie zunächst FTP im Bereich mit den Dateiübertragungseinstellungen auf der Registerkarte „FTP“ aktivieren.

Um mehrere Dateien in einem Vorgang zu übertragen, verwenden Sie die Option **Batch**.

1. Aktivieren Sie unter „Einstellungen“ > „Dateiübertragung“ > „FTP“ die Option **FTP aktivieren**.
2. Klicken Sie auf FTP BATCH, um den Bereich für die Batchdateiübertragung zu öffnen.
3. Wählen Sie „Batch bei einzelnem Fehler abbrechen“ aus, um die Übertragung zu beenden, wenn eine Datei nicht übertragen werden kann.
4. Klicken Sie auf +, um die Liste der zu übertragenden Dateien zu erstellen.

   a. Benennen Sie die Liste. Zur Erstellung ähnlicher Listen können Sie eine vorhandene Liste kopieren, diese umbenennen und dann mithilfe der Optionen, die verfügbar sind, wenn die ursprüngliche Liste markiert wird, nach Bedarf Dateien hinzufügen oder löschen.

   b. Klicken Sie im rechten Bereich auf +, um das Dialogfeld „Übertragungsanforderung hinzufügen“ zu öffnen.
5. Erstellen Sie im Bereich „Übertragungsanforderung hinzufügen“ die Liste:

Option	Beschreibung
Übertragung	Wählen Sie aus, ob die Datei hoch- oder heruntergeladen werden soll.
Name der lokalen Datei	Geben Sie die Datei an, die übertragen werden soll. Sie können den Namen der Datei eingeben oder zu der Datei navigieren.
Pfad der Remotedatei	Geben Sie ein Verzeichnis an, in dem die Datei nach der Übertragung benannt und gespeichert wird. Sie haben folgende Möglichkeiten: • **Beibehalten des ursprünglichen Dateinamens und Verwenden des ursprünglichen Remoteverzeichnisses**: Lassen Sie das Feld leer. • **Verwenden eines neuen Dateinamens**: Geben Sie „neuerdateiname.txt“ ein. Die Datei wird unter dem angegebenen Namen im ursprünglichen Remoteverzeichnis gespeichert. • **Beibehalten des ursprünglichen Dateinamens und Verwenden eines neuen Verzeichnispfads**: `/folder/`. Der ursprüngliche Dateiname wird mit dem neuen Pfad verwendet. • **Verwenden eines neuen Verzeichnisses und eines neuen Dateinamens**: `/folder/newfilename.txt`.
Übertragungsart	Sie können die Übertragungsart „Binär“ oder „ASCII“ auswählen.
Falls Remotedatei vorhanden	

Legen Sie fest, wie die Dateiübertragung erfolgen soll, wenn bereits eine Remotedatei vorhanden ist. Die Optionen sind:

- Überschreiben (Standard): Die auf dem Remotecomputer bereits vorhandene Datei wird überschrieben.
- Anfügen: Die gesendete Datei wird an die vorhandene Datei angefügt.
- Benutzer fragen (Standard): Es wird gefragt, wie mit dem doppelten Dateinamen zu verfahren ist.
- Abbrechen: Die Dateiübertragung wird abgebrochen.
- Fehler: Die Dateiübertragung wird abgebrochen, und eine Fehlerbenachrichtigung wird gesendet.
- Überspringen: Die Datei, deren Name mit einem vorhandenen Dateinamen übereinstimmt, wird übersprungen, die Übertragung der anderen Dateien im Batch wird jedoch fortgesetzt.
- Eindeutig: Eine neue Datei mit einem eindeutigen Dateinamen wird erstellt.

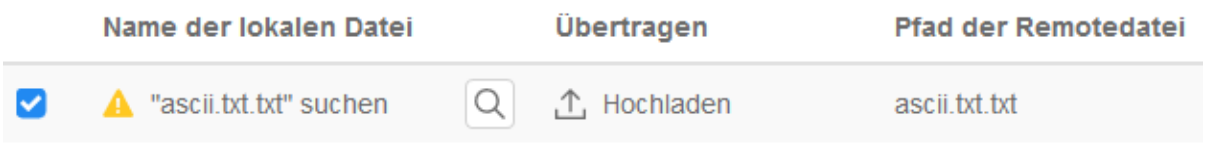
1. Klicken Sie auf **Speichern**.

Dateien übertragen (Batch)

> **Tipp**
>
> Administratoren erteilen über die Option **Regeln für Benutzereinstellungen** im Bereich „Einstellungen“ die Berechtigung zum Übertragen von Dateien.

Klicken Sie in der Symbolleiste auf  , um die Liste zu öffnen, die die zu übertragenden Dateien enthält.

1. Aufgrund von Browseranforderungen müssen Sie das Verzeichnis aller Dateien angeben, die hochgeladen werden sollen. Suchen Sie die entsprechenden Dateien bei Bedarf über das Suchsymbol. Diese Dateien lassen sich wie im Beispiel in der folgenden Abbildung leicht anhand eines gelben Symbols erkennen:



2. Die Dateien in der Batchliste sind standardmäßig ausgewählt. Um Dateien vor der Übertragung zu bearbeiten, können Sie Dateien vom Übertragungsvorgang ausschließen, indem Sie die entsprechenden Kontrollkästchen deaktivieren oder im Dropdownmenü die Option **Alle** auswählen. Zudem können Sie die Liste der übertragbaren Dateien basierend auf dem zugehörigen Download- oder Uploadstatus filtern.
3. Klicken Sie auf **Starten**, um die Übertragung zu starten.

5.5 Angeben von Bearbeitungsoptionen

Bearbeitungsoptionen für verschiedene Kopier-, Einfüge- und Ausschneidevorgänge.

Kopieroptionen

Markieren Sie Text, indem Sie die linke Maustaste gedrückt halten und den Mauszeiger über den Text bewegen oder indem Sie die Umschalttaste gedrückt halten und die Auswahl mit den Pfeiltasten ändern. Standardmäßig verwenden verschiedene Terminaltypen beim Kopieren von Text unterschiedliche Auswahlmodi. VT-Terminals verwenden einen linearen Auswahlmodus, während alle anderen Terminals die Blockmodusauswahl verwenden. Um auf einem beliebigen Terminaltyp zwischen den Auswahlmodi zu wechseln, halten Sie die **Alt**-Taste gedrückt und wählen Sie den gewünschten Text aus.

- Nur Eingabefelder kopieren – Wählen Sie diese Option, um nur Daten aus Eingabefeldern zu kopieren. Daten aus geschützten Feldern werden beim Hinzufügen zur Zwischenablage durch Leerzeichen ersetzt.
- Gesamte Anzeige verwenden, wenn keine Auswahl getroffen ist – Diese Option wendet den Befehl „Kopieren“ auf die gesamte Terminalanzeige an, wenn nichts ausgewählt wurde.

Einfügeoptionen

Wählen Sie „Einfügen“, um den Inhalt der Zwischenablage an der Cursorposition einzufügen.

- **Geschützte Felder überspringen** – Gibt an, wie der eingefügte Text auf dem Bildschirm angezeigt wird:
  - Wenn dieses Kontrollkästchen deaktiviert ist (Standardeinstellung), wird der Text als linearer Datenstrom, der neue Zeilen und Trennzeichen enthalten kann, interpretiert und entsprechend eingefügt.
  - Wenn dieses Kontrollkästchen aktiviert ist, wird der Text als Daten des Hostbildschirms interpretiert und bei der aktuellen Cursorposition über den aktuellen Bildschirm gelegt. Bei einem ungeschützten Feld im Bildschirm wird der Quelltext eingefügt, bei einem geschützten Feld im Bildschirm wird der Quelltext übersprungen.
- **In nächstes Feld in der aktuellen Zeile umbrechen** – Wählen Sie diese Option aus, damit aus der Zwischenablage eingefügte Daten das aktuelle Feld so weit wie möglich ausfüllen. Alle verbleibenden Daten werden in das nächste Feld in derselben Zeile eingefügt, bis das Ende der Zeile erreicht ist oder alle Daten eingefügt wurden. Wenn **In nächste Zeile umbrechen** ebenfalls ausgewählt ist, werden die ggf. dann noch verbleibenden Daten in die anschließenden Felder in der nächsten Zeile eingefügt und die Daten werden vertikal an der Anfangsposition des Cursors ausgerichtet.
- **In nächste Zeile umbrechen** – Wenn diese Option aktiviert ist, füllt der Einfügebefehl das erste Feld mit so vielen Zwischenablagedaten aus, wie das Feld fassen kann. Der verbleibende Text wird in die Zeile direkt darunter eingefügt, vorausgesetzt, sie ist beschreibbar (z. B. ein Eingabefeld). Andernfalls wird der verbleibende Text abgeschnitten. Nachfolgende Datenzeilen werden so eingefügt, dass sie vertikal an der Anfangsposition des Cursors ausgerichtet sind.

  Standardmäßig ist diese Option nicht ausgewählt und Text, der über das Feld hinausgeht, wird abgeschnitten.
- **Anfangscursorposition nach dem Einfügen wiederherstellen** – Standardmäßig befindet sich der Hostcursor nach einem Einfügevorgang am Ende der Daten. Aktivieren Sie diese Option, um den Hostcursor nach Abschluss des Einfügevorgangs an die Anfangsposition zurückzusetzen.

Ausschneideoptionen

Der Ausschneidevorgang ist für alle unterstützten Terminals außer VT-Hosttypen verfügbar. Wählen Sie den Bereich aus, den Sie ausschneiden möchten, und klicken Sie dann auf die Schaltfläche  in der Symbolleiste. Sie können entweder das Kontextmenü oder die Tastenkombination verwenden, um die Daten auf dem Bildschirm auszuschneiden und in der Zwischenablage zu speichern. Daten in geschützten Feldern werden in die Zwischenablage kopiert, aber nicht vom Bildschirm entfernt.

Tastenkombinationen

HACloud unterstützt gängige Tastenkombinationen für Bearbeitungsfunktionen. Diese Tasten werden an den Browser geleitet, der die entsprechenden Bearbeitungsfunktionen generiert.

Tastenkombination	Hosttyp	Aktion
Strg+C	3270, 5250, UTS, T27 und ALC	Kopieren
Strg+V	3270, 5250, UTS, T27 und ALC	Einfügen
Strg+X	3270, 5250, UTS, T27 und ALC	Ausschneiden

Diese Tastenkombinationen sind in HACloud verschiedenen Bildschirmbearbeitungsaktionen zugeordnet:

Tastenkombination	Hosttyp	Aktion
Strg+A	3270, 5250, UTS, T27, ALC	Gesamten Text auf dem Bildschirm auswählen
Umschalt+Pfeiltaste	Alle	Umfang der aktuellen Auswahl ändern
Strg+Umschalt+A	VT	Alles auswählen
Strg+Umschalt+C	VT	Kopieren
Strg+Umschalt+V	VT	Einfügen

Hinweis

In HACloud können Sie mit der Tastenzuordnungsfunktion Bearbeitungsaktionen bestimmten Tastenkombinationen zuzuordnen. Sie können über ein Kontextmenü im Terminal auf die Bearbeitungsaktionen zugreifen, indem Sie mit der rechten Maustaste auf den Bildschirm klicken. Die Bearbeitungsaktionen können durch Browserberechtigungen eingeschränkt sein. Wenn eine Aktion für den Benutzer nicht verfügbar ist, werden die zugehörigen Symbolleistenschaltflächen und Kontextmenüelemente nicht angezeigt.

Weitere Informationen

Bearbeiten des Bildschirms

5.6 Verwenden von Sitzungen

Alle Sitzungen, auf die Sie zugreifen können, sind in der Liste „Verfügbare Sitzungen“ enthalten. Sitzungen werden anfänglich vom Systemadministrator erstellt und konfiguriert und können über eine verteilte URL (z. B. `https://<Sitzungsserver>:7443/`) abgerufen werden.

So öffnen Sie eine Sitzung

1. Klicken Sie auf die gewünschte Sitzung, um sie zu öffnen.

2. Interagieren Sie über die geöffnete Sitzung mit der Hostanwendung.

3. Sie können mehrere Instanzen einer konfigurierten Sitzung erstellen.

Sie können gleichzeitig mehrere Sitzungen öffnen und über die oben am Bildschirm angeordneten Registerkarten problemlos zwischen den Sitzungen wechseln. Die aktuelle Sitzung befindet sich immer auf der äußeren linken Registerkarte und wird mit einem weißen Hintergrund und als fett formatierter Text angezeigt. Jede Sitzung bleibt 30 Minuten lang im aktiven Modus.

Bei der Interaktion mit der Sitzung haben Sie über die Symbolleiste Zugriff auf die verschiedenen verfügbaren Optionen. Sie können die Verbindung mit einer Sitzung trennen, die Sitzung schließen, „Kurztasten“ aktivieren und auf weitere Einstellungen zugreifen. Einige dieser Optionen sind nur verfügbar, wenn Ihr Administrator entsprechende Genehmigungen erteilt hat.

5.6.1 Arbeiten mit Kurztasten

„Kurztasten“ ist eine Terminaltastatur für die grafische Darstellung von Tasten auf einer Hosttastatur, mit der Sie schnell auf Terminaltasten zugreifen können.

Durch Klicken auf eine Terminaltaste der Kurztasten-Tastatur können Sie die Taste an den Host senden. Mit QuickInfos, die durch Bewegen des Mauszeigers über eine Taste verfügbar sind, wird eine Beschreibung der Zuordnung angezeigt.

Für jeden unterstützten Hosttyp sind Kurztasten verfügbar, auf die Sie durch Klicken auf das Symbol  in der Symbolleiste zugreifen können.

5.6.2 Bearbeiten des Bildschirms

> **Hinweis**
>
> Das Kopieren, Einfügen und Ausschneiden wird in jedem Browser auf unterschiedliche Weise gehandhabt und nicht jeder Browser unterstützt die Verwendung der Schaltflächen in der Symbolleiste und der entsprechenden Befehle im Kontextmenü. Um diese Funktionen möglichst praktisch zu nutzen, sollten Sie Tastaturbefehle verwenden. Die Belegung der Tastaturbefehle kann je nach Betriebssystem voneinander abweichen. Unter Windows lautet sie: STRG+C zum Kopieren, STRG+V zum Einfügen und STRG+X zum Ausschneiden.
>
> Mit der Funktion zum Einfügen treten deutlich häufiger Probleme auf als mit der Ausschneide- oder Kopierfunktion. Wenn die Schaltfläche zum Einfügen nicht in der Symbolleiste angezeigt wird, verhindern möglicherweise die Browsersicherheitseinstellungen den Lesezugriff auf die Zwischenablage des Systems. Der Zugriff auf die Zwischenablage wird in jedem Browser anders gehandhabt. Die Funktion zum Einfügen ist jedoch fast immer über eine Tastenkombination verfügbar (Strg+V unter Windows bzw. Befehlstaste+V unter Mac). Voraussetzung ist, dass Sie diese Tasten nicht neu zugeordnet haben. Alternativ können Sie die integrierten Menüeinträge oder Schaltfläche im Browser zum Einfügen verwenden.

So kopieren Sie Inhalte aus dem Terminal

1. Markieren Sie auf dem Terminalbildschirm den Bereich, der kopiert werden soll.
2. Klicken Sie in der Symbolleiste auf **Kopieren** oder wählen Sie im Kontextmenü, das über das Terminalfenster verfügbar ist, **Kopieren** aus. Alternativ können Sie die Tastenkombination **STRG+V** verwenden.

So fügen Sie Inhalte in den Terminalbildschirm ein

1. Bewegen Sie den Cursor zu der Position, an der Sie Inhalte einfügen möchten.
2. Wenn der Browser die Funktion zum Einfügen unterstützt, klicken Sie in der Symbolleiste auf **Einfügen** oder wählen Sie im Kontextmenü im Terminalfenster den Eintrag **Einfügen** aus. Wenn der Browser diese Funktion nicht unterstützt, sind diese Optionen nicht verfügbar. Verwenden Sie in diesem Fall die Tastenkombination **STRG+V**.

So schneiden Sie Bereiche vom Terminalbildschirm aus

> **Hinweis**
>
> Diese Funktion ist für alle unterstützten Terminaltypen mit Ausnahme von VT-Hosts verfügbar.

1. Markieren Sie auf dem Terminalbildschirm den Bereich, der ausgeschnitten werden soll.
2. Klicken Sie in der Symbolleiste auf **Ausschneiden** oder wählen Sie im Kontextmenü, das über das Terminalfenster verfügbar ist, **Ausschneiden** aus. Alternativ können Sie die Tastenkombination **STRG+X** verwenden.

Weitere Informationen

- Angeben von Bearbeitungsoptionen

5.6.3 Abmelden

Öffnen Sie am oberen rechten Rand des Bildschirms die Dropdown-Liste neben Ihrem Benutzernamen und wählen Sie **Abmelden** aus, um die Arbeit in der Hostanwendung zu beenden.

5.7 Erstellen von Makros

Ein Makro ist eine Folge von Tastatureingaben, die Sie aufzeichnen und ausführen können. Diese JavaScript-Makroprogramme werden für die Automatisierung von Interaktionen mit dem Terminal verwendet. Sie können mit allen unterstützten Geräten auf Makros zugreifen und sie ausführen.

Die Makros werden von Host Access for the Cloud als JavaScript aufgezeichnet und gespeichert, sodass Sie die aufgezeichneten Makros problemlos bearbeiten und ergänzen können. Sie können Makros für eine spätere Wiedergabe aufzeichnen oder Makros beim Programmstart und beim Verbinden bzw. Trennen der Verbindung zum Host ausführen lassen. Sie können Makros auch ganz neu schreiben, um komplexere Aufgaben auszuführen, die das Aufzeichnungsprogramm nicht erfassen kann.

Makros werden Benutzern auf zwei unterschiedliche Arten zur Verfügung gestellt: Sie werden von einem Administrator erstellt oder von Benutzern für ihre eigene persönliche Verwendung aufgezeichnet. Alle erweiterten Makros sind einer Sitzung zugeordnet und haben mit der Automatisierung der Hostinteraktion alle das gleiche Ziel. Der einzige Unterschied zwischen den beiden Bereitstellungsmethoden ist der Zugriff auf die Makros und die Verwaltung der Erstellung und Verfügbarkeit.

- **Durch Administratoren erstellte Makros**

  Administratoren zeichnen Makros beim Erstellen der Sitzung auf. Die Makros gelten für eine bestimmte Sitzung und stehen allen Benutzern zur Verfügung, die über das Makro-Symbol in der Symbolleiste Zugriff auf die Sitzung haben. Administratoren können Makros für eine Wiedergabe beim Programmstart oder beim Verbinden bzw. Trennen der Verbindung zum Host zuweisen.

- **Durch Benutzer erstellte Makros**

  Endbenutzermakros werden von Einzelpersonen für die Sitzungen erstellt, zu denen ihnen Zugriff gewährt wurde. Administratoren erteilen die Genehmigung für die Erstellung von Makros, indem Sie eine Regel für Benutzereinstellungen erstellen. Die Benutzer können mit dem eigenen Berechtigungsnachweis oder über eine Gastrolle auf die Sitzung zugreifen. Makros, die von Gastbenutzern erstellt werden, stehen auch allen anderen Gastbenutzern zur Verfügung. Wenn sich Benutzer mit ihren Anmeldeinformationen anmelden, werden ihnen nur die selbst erstellten Makros angezeigt.

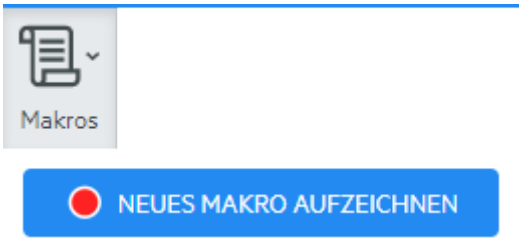
  Erweiterte Makros werden in alphabetischer Reihenfolge in der Dropdownliste aufgelistet, die in der Symbolleiste abgerufen werden kann. Die von Endbenutzern erstellten Makros werden am Anfang der Liste angezeigt, gefolgt von einem aus drei grauen vertikalen Punkten bestehenden Symbol, das bei Auswahl die Optionen „Bearbeiten“ und „Löschen“ anzeigt. Die von Administratoren erstellten Makros werden hingegen ohne das Symbol angezeigt, da derartige Makros von Endbenutzern nicht angepasst werden können.

5.7.1 Arbeiten mit Makros

Führen Sie die folgenden Schritte aus, um Makros aufzuzeichnen, zu bearbeiten und auszuführen.

Aufzeichnen

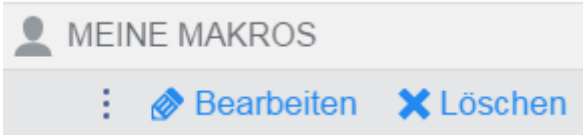
1. Klicken Sie in der Symbolleiste zunächst auf das Makrosymbol und anschließend auf „Neues Makro aufzeichnen“.

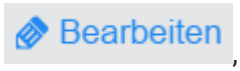


2. Navigieren Sie durch die Hostanwendung, um die Schrittfolge aufzuzeichnen, die im Makro enthalten sein soll.
3. Klicken Sie in der Symbolleiste auf  , um die Aufnahme anzuhalten. Der rote Punkt blinkt und zeigt somit an, dass die Aufzeichnung gerade durchgeführt wird.
4. Wenn Sie dazu aufgefordert werden, geben Sie dem Makro einen Namen.

Bearbeiten

1. Wählen Sie aus der Dropdown-Liste „Makro“ das zu bearbeitende Makro aus.



2. Klicken Sie auf die drei vertikalen Punkte, um das Feld zu erweitern.
3. Klicken Sie auf  , um den Makroeditor zu öffnen (im linken Bereich).
4. Nehmen Sie mit JavaScript die gewünschten Änderungen vor. Sie können das angepasste Makro über die Symbolleistensymbole im oberen Bereich des Editors ausführen und speichern.

Führen Sie

Um ein Makro auszuführen, wählen Sie es aus der Dropdown-Liste aus und klicken Sie auf  .

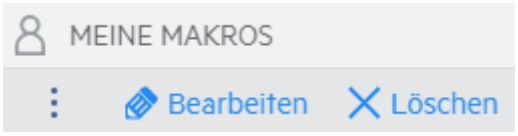
Sie können auch Tasten zuordnen, über die ein bereits aufgezeichnetes Makro automatisch ausgelöst wird. Wählen Sie im Dialogfeld „Tastenbelegungen“ in der Dropdownliste **Aktion** die Option **Makro ausführen** aus. Wählen Sie in der Liste **Wert** ein Makro aus, das der Tastenbelegung zugeordnet werden soll.

Stoppen

Sie können ein Makro jederzeit vor Abschluss über den Makroeditor oder die Symbolleiste anhalten. Klicken Sie auf  , um ein Makro anzuhalten. Wenn Sie das Makro erneut ausführen möchten, kehren Sie zum Makro-Startbildschirm zurück.

Löschen

1. Wählen Sie aus der Dropdown-Liste „Makro“ das zu löschende Makro aus.
2. Erweitern Sie das Feld, indem Sie auf das Symbol mit den drei vertikalen Punkten klicken.



3. Klicken Sie auf **Löschen**.

Anzeigen

Die Dropdown-Liste „Makro“ steht in der Symbolleiste allen Benutzern zur Verfügung, die zum Aufzeichnen von Makros berechtigt sind oder auf eine Sitzung zugreifen, in der Makros vorab von einem Administrator zur Verwendung in der entsprechenden Sitzung aufgezeichnet wurden.

Makros werden, je nachdem, wie sie aufgezeichnet wurden, unter **MEINE MAKROS** oder **MAKROS** aufgelistet.

Die der Sitzung zugewiesenen Makros werden allen Benutzern angezeigt. Dies ist unabhängig davon, ob sich die Benutzer mit dem eigenen Berechtigungsnachweis oder als Gast angemeldet haben. Die unter **MEINE MAKROS** aufgelisteten Makros sind in alphabetischer Reihenfolge nach Name sortiert und sind für die Benutzer sichtbar, die die Makros aufgezeichnet haben. Makros, die von einem Administrator aufgezeichnet und zu einer Sitzung hinzugefügt wurden, sind in alphabetischer Reihenfolge unter **MAKROS** aufgelistet.

5.7.2 Fehlersuche für Makros

Makros werden in JavaScript geschrieben und im Browser ausgeführt. Daher sollte die Fehlersuche mit den in den Webbrowsern integrierten Werkzeugen durchgeführt werden. Moderne Browser sind mit einer Reihe äußerst wirksamer Werkzeuge zur Fehlersuche in JavaScript-Code ausgestattet. Sie können damit Haltepunkte positionieren, sich durch Code bewegen und Debug-Informationen ausgeben.

> **Tipp**
>
> In JavaScript wird die Groß-/Kleinschreibung beachtet. Achten Sie darauf, wenn Sie JavaScript-Code bearbeiten.

So führen Sie eine Fehlersuche für ein Makro aus:

1. Öffnen Sie das Makro zur Bearbeitung. Anweisungen finden Sie unter Arbeiten mit Makros.
2. Öffnen Sie die Entwicklungswerkzeuge Ihres Browsers.

Browser	Debugger öffnen
Mozilla Firefox 40.0.3	• Öffnen Sie über die Symbolleiste das Menü, und wählen Sie „Entwickler“ aus. • Wählen Sie aus dem Menü „Web-Entwickler“ den Eintrag „Debugger“. Der Debugger wird im unteren Bereich geöffnet.
Google Chrome 45.0	• Öffnen Sie über die Symbolleiste das Menü, und wählen Sie „Weitere Tools“ aus. • Wählen Sie „Entwicklungstools“, um den Debugger zu öffnen.
Microsoft Internet Explorer 11	• Öffnen Sie über die Symbolleiste die „Einstellungen“, und wählen Sie „F12-Entwicklungstools“. • Öffnen Sie die Registerkarte „Debugger“.

3. Verwenden Sie eines dieser Werkzeuge im Makrocode und führen Sie den Code aus.

   - debugger

     Den gründlichsten Ansatz für die Fehlersuche stellt die Anweisung `'debugger;'` dar. Wenn Sie diese Anweisungen in den Makrocode einfügen und den Makrocode ausführen, während die Entwicklungswerkzeuge des Browsers geöffnet sind, wird die Ausführung an diesen Zeilen angehalten. Sie können das Makro schrittweise ausführen und den Wert der lokalen Variablen sowie weitere zu prüfende Werte anzeigen.

     Sie sollten mehrere 'debugger;'-Anweisungen im Code platzieren, um zur richtigen Zeile zu gelangen. Aufgrund der asynchronen Eigenschaft von JavaScript kann die schrittweise Ausführung von Code herausfordernd sein. Wenn Sie mehrere 'debugger;'-Anweisungen sorgfältig platzieren, können Sie diese Effekte jedoch abmildern.

     Beispiel 1: `debugger`

     ```
     var hostCommand = menuSelection + '[enter]';
     debugger; // <– Der Debugger des Browsers wird hier anhalten
     ps.sendKeys(hostCommand);
     ```

   - console.log(), alert()

     Diese beiden Funktionen werden häufig für die Fehlersuche in JavaScript verwendet. Sie sind nicht so flexibel wie eine 'debugger;'-Anweisung, bieten aber die Möglichkeit, Debug-Informationen schnell auszugeben. Diese Funktionen geben die Informationen an die JavaScript-Registerkarte „Konsole“ in den Entwicklungswerkzeugen des Browsers aus.

     Beispiel 2: `console.log(), alert()`

     ```
     var hostCommand = menuSelection + '[enter]';
     console.log('Command:' + hostCommand); // <– Gibt die Zeichenkette an die Registerkarte
   "Console" aus
     alert('Command:' + hostCommand); // Öffnet ein kleines Fenster mit den Daten
     ps.sendKeys(hostCommand);
     ```

   - ui.message()

     Die Host Access for the Cloud-Makro-API bietet eine ui.message()-Funktion, die der JavaScript-Funktion alert() sehr ähnelt. Sie können „ui.message()“ auch zum Ausgeben von Debug-Informationen verwenden.

     Beispiel 3: `ui.message()`

     ```
     var hostCommand = menuSelection + '[enter]';
     ui.message('Command:' + hostCommand); // <– Zeigt ein Meldungsfenster an
     ps.sendKeys(hostCommand);
     ```

Beachten Sie Folgendes:

- Schrittweise Ausführung und „yields“

  Die yield-Anweisungen tragen zwar zum besseren Verständnis von Makros bei, können jedoch die schrittweise Ausführung des Codes mit dem Debugger erschweren. Daher sollten Sie entweder mehrere debugger-Anweisungen oder sorgfältig platzierte debugger-Anweisungen von `console.log()`-Aufrufen verwenden, um die richtigen Debug-Informationen auszugeben.

- Internet Explorer

  Die Fehlersuche in Internet Explorer beinhaltet umgewandelten Code und kann herausfordernder sein als die Fehlersuche in anderen Browsern.

5.7.3 Verwenden der Makro-API

Makros werden in Host Access for the Cloud mit JavaScript aufgezeichnet und geschrieben.

Die Makro-API setzt sich aus einer Reihe von Objekten zusammen, über die Sie mit dem Host interagieren, auf Bildschirmstatus warten und mit dem Benutzer interagieren können.

Informationen zu „promises“ und „yields“

Da JavaScript in einem einzelnen Thread läuft und für die Verwaltung der Ausführung „callback“-Funktionen und „promises“ verwendet, ist der Code möglicherweise schwer nachvollziehbar. Host Access for the Cloud verbindet das Konzept von „Zusagen“ mit dem „yield“-Schlüsselwort, damit Makrocode linear organisiert werden kann.

- **Promises**

  Promises sind Muster zur Vereinfachung von Funktionen, die an einem in der Zukunft liegenden Punkt Ergebnisse asynchron zurückgeben. Alle Funktionen der Typen „wait“ und „ui“ in der Makro-API geben „promise“-Objekte zurück.

- **Yield**

  Makros verwenden das „yield“-Schlüsselwort, um die Ausführung des Makros zu blockieren, bis ein „promise“-Objekt aufgelöst oder ausgeführt wurde. Wenn also 'yield' vor einer beliebigen 'wait'- oder 'ui'-Funktion gesetzt wird, wird die Ausführung des Makros angehalten, bis die Ausführung dieser Funktion abgeschlossen ist. Sie können das 'yield'-Schlüsselwort vor jeder Funktion platzieren, die 'promise' zurückgibt, also auch für Ihre benutzerdefinierten Funktionen.

> **Hinweis**
>
> Die Funktion zum Blockieren der Makroausführung durch die Kombination von „yield“ und „promises“ wird in der Funktion `createMacro()` aktiviert.

Fehlermeldungen

Fehler werden in Makros mithilfe der 'try / catch'-Anweisung behandelt. Einige der API-Funktionen können Fehler ausgeben, wenn beispielsweise Bedingungen nicht erfüllt werden können oder eine Zeitüberschreitung eintritt. Der ausgegebene Fehler wird in die 'catch'-Anweisung aufgenommen. Sie können kleinere Codeblöcke in einer „try / catch“-Anweisung umbrechen, um Fehler detaillierter zu behandeln.

Entwickler von Makros können Fehler auch über `'throw new Error('Hilfreiche Fehlermeldung');` ausgeben.

Weitere Informationen

- Makro-API-Objekte
- Beispielmakros

5.8 Makro-API-Objekte

Sie können Makros mithilfe der Makro-API erstellen. Für die standardmäßige Verwendung in Makros stehen vier primäre Objekte zur Verfügung:

- **Session** – der Haupteinstiegspunkt zum Host. Mit dem Session-Objekt stellen Sie eine Verbindung zum PresentationSpace-Objekt her, trennen die Verbindung zu diesem Objekt und gewähren Zugriff darauf.
- **PresentationSpace** – stellt den Bildschirm dar und bietet zahlreiche allgemeine Funktionen wie das Abrufen und Festlegen der Cursorposition, das Senden von Daten an den Host und das Lesen auf dem Bildschirm. Dieses Objekt wird mit `session.getPresentationSpace()` abgerufen.
- **Wait** – bietet eine einfache Möglichkeit, auf das Auftreten der verschiedenen Hoststatus zu warten, bevor weitere Daten gesendet oder auf dem Bildschirm gelesen werden. Sie können beispielsweise darauf warten, dass sich der Cursor an einer bestimmten Position befindet, dass Text an einer bestimmten Position des Bildschirms angezeigt wird oder einfach für eine festgelegte Zeit. Alle Aufrufe der Funktion 'Wait' erfordern das 'yield'-Schlüsselwort, das weiter unten beschrieben wird.
- **User Interface** – automatisch in Ihrem Makro als die Variable „ui“ verfügbar. Es stellt die grundlegenden Funktionen der Benutzeroberfläche bereit. Mit diesem Objekt werden dem Benutzer Daten angezeigt oder Informationen abgefragt. Alle Aufrufe der Funktion 'ui' erfordern das yield-Schlüsselwort.

Alle verfügbaren Objekte

Die Liste der verfügbaren Objekte können Sie in der rechten Navigation unter „Auf dieser Seite“ anzeigen. (Möglicherweise müssen Sie Ihren Browser erweitern.)

5.8.1 Attribut

Verwenden Sie das Attribute-Objekt gemeinsam mit dem AttributeSet-Objekt zum Decodieren der Formatierungsinformationen in der Datenzelle.

Attribut	Bedeutung
PROTECTED	geschützte Datenzelle
MODIFIED	geänderte Datenzelle
NUMERIC_ONLY	Anfang einer ausschließlich numerischen Datenzelle
ALPHA_NUMERIC	alphanumerische Datenzelle
HIGH_INTENSITY	ob die Datenzelle Text mit hoher Intensität enthält
HIDDEN	ob die Datenzelle ausgeblendeten Text enthält
PEN_DETECTABLE	ob die Datenzelle von Stiften erkannt wird
ALPHA_ONLY	ausschließlich alphanumerische Datenzelle
NUMERIC_SHIFT	Anfang eines numerischen Umschaltfelds
NUMERIC_SPECIAL	Datenzelle markiert den Anfang eines numerischen Sonderfelds
KATAKANA_SHIFT	Abschnitt mit Katakana-Text
MAGNETIC_STRIPE	Datenzelle markiert den Anfang eines Magnetstreifenfelds
SIGNED_NUMERIC_ONLY	Datenzelle ist ein Feld für numerische Daten mit Vorzeichen
TRANSMIT_ONLY	Datenzelle ist ein Feld nur für die Übertragung
FIELD_END_MARKER	Datenzelle markiert das Ende eines geänderten Felds
FIELD_START_MARKER	Datenzelle markiert den Anfang eines geänderten Felds
SPECIAL_EMPHASIS_PROTECTED	geschütztes Feld mit besonderer Hervorhebung
TAB_STOP	Datenzelle enthält einen Tabstopp
REVERSE	Datenzelle wird in umgekehrter Darstellung angezeigt
BLINKING	Datenzelle enthält blinkenden Text
RIGHT_JUSTIFIED	Datenzelle markiert den Anfang eines rechts ausgerichteten Felds

Attribut	Bedeutung
LEFT_JUSTIFIED	Datenzelle markiert den Anfang eines links ausgerichteten Felds
LOW_INTENSITY	Datenzelle enthält Text mit niedriger Intensität
UNDERLINE	Datenzelle enthält unterstrichenen Text
DOUBLE_BYTE	Datenzelle enthält Doppelbyte-Text
COLUMN_SEPARATOR	Datenzelle enthält ein Spaltentrennzeichen
BOLD	Datenzelle enthält fett formatierten Text
DOUBLE_WIDTH	Datenzelle enthält ein Feld mit doppelter Breite
DOUBLE_HEIGHT_TOP	Datenzelle mit doppelter oberer Höhe
DOUBLE_HEIGHT_BOTTOM	Datenzelle mit doppelter unterer Höhe
CONTROL_PAGE_DATA	Datenzelle enthält Steuerungsseitendaten
RIGHT_COLUMN_SEPARATOR	Datenzelle enthält ein rechtes Spaltentrennzeichen
LEFT_COLUMN_SEPARATOR	Datenzelle enthält ein linkes Spaltentrennzeichen
UPPERSCORE	Datenzelle enthält einen Überstrich
STRIKE_THROUGH	Datenzelle enthält durchgestrichenen Text

5.8.2 AttributeSet

Mit dem AttributeSet-Objekt können Benutzer die in der Datenzelle enthaltenen Attribute decodieren. Das AttributeSet-Objekt gibt die im Attribute-Objekt definierten Werte zurück. Wenn sie

gemeinsam verwendet werden, können Sie die Formatierungsinformationen aus der Datenzelle abrufen.

Methode	Beschreibung
`contains(attribute)`	Gibt an, ob der Satz das festgelegte Attribut (attribute) enthält. **Parameter** `{Number}` Zu prüfendes Attribut. **Rückgabe** `{Boolean}` „True“ (wahr), wenn das Attribut im Satz enthalten ist.
`isEmpty()`	Gibt an, ob der Attributsatz leer ist. **Rückgabe** `{Boolean}` „True“ (wahr), wenn der Satz leer ist.
`size()`	Gibt die Anzahl der in einem Satz enthaltenen Attribute an. **Rückgabe** `{Number}` Die Attributanzahl.
`toArray()`	Konvertiert den internen Attributsatz in ein Array. **Rückgabe** `{Number[]}` Array mit den Werten der Attribute im Satz.
`toString()`	Konvertiert den internen Attributsatz in eine Zeichenfolge. **Rückgabe** `{String} Durch Leerzeichen getrennte Namen der im Satz enthaltenen Attribute.`
`forEach(callback, thisArg)`	Funktion zum Durchlaufen der einzelnen Elemente im Attributsatz. **Parameter** `{forEachCallback}` Callback zum Ausführen eines bestimmten Vorgangs. Wird gemeinsam mit dem Namen des jeweiligen Attributs im Satz aufgerufen. `{Object} thisArg` Optionaler Verweis auf ein Kontextobjekt.
`forEachCallback(string, object)`	Eine durch Benutzer bereitgestellte Rückruffunktion, mit der Sie das Verhalten bereitstellen. Wird als Rückrufparameter für 'forEach' verwendet. **Parameter** `{String} Zeichenkettenname eines Attributs im Attributsatz.`

`{Object} thisArg` Optionaler Verweis auf ein Kontextobjekt.

5.8.3 AutoSignOn

Methode	Beschreibung
`getPassTicket()`	Ruft ein Weiterleitungsticket ab, das für die Anmeldung bei einer Mainframe-Anwendung verwendet werden soll. Unter Verwendung verschiedener Anwendungskennungen können mehrere Weiterleitungstickets angefordert werden. **Parameter** {String} Anwendungs-ID, die dem Host mitteilt, für welche Anwendung die Anmeldung gilt. **Rückgabe** {Promise} Erfüllt mit Weiterleitungsticketschlüssel bzw. abgelehnt, wenn der Vorgang nicht ausgeführt werden kann. Das vom DCAS abgerufene Weiterleitungsticket kann nur mit der aktuellen Hostsitzung verwendet werden und ist für zehn Minuten gültig.
`sendUserName()`	Wendet den im Weiterleitungsticket enthaltenen Benutzernamen auf das Feld an der aktuellen Cursorposition auf dem aktuellen Hostbildschirm an. Der Benutzername muss vor dem Passwort gesendet werden. Wenn Sie das Passwort zuerst senden, wird das Weiterleitungsticket ungültig, und Sie müssen ein neues Ticket anfordern. **Parameter** {String} Mit „getPassTicket“ abgerufener Weiterleitungsticketschlüssel (passTicketKey). **Rückgabe** {Promise} Erfüllt, wenn der Benutzername erfolgreich gesendet wurde. Wird abgelehnt, wenn der Vorgang fehlschlägt.
`sendPassword()`	Wendet das im Weiterleitungsticket enthaltene Passwort auf das Feld an der aktuellen Cursorposition auf dem aktuellen Hostbildschirm an. Der Benutzername muss vor dem Passwort gesendet werden. Wenn Sie das Passwort zuerst senden, wird das Weiterleitungsticket ungültig, und Sie müssen ein neues Ticket anfordern. **Parameter** {String} Mit „getPassTicket“ abgerufener Weiterleitungsticketschlüssel (passTicketKey). **Rückgabe** {Promise} Erfüllt, wenn das Passwort erfolgreich gesendet wurde. Abgelehnt, wenn der Vorgang nicht ausgeführt werden kann.

5.8.4 Farbe

Farbkonstanten zur Verwendung für die Vordergrund- und Hintergrundfarben von DataCell-Objekten.

Farbe	Beschreibung	Numerischer Wert
BLANK_UNSPECIFIED	Keine Farbe angegeben	0
BLUE	Blau	1
GREEN	Grün	2
CYAN	Cyan	3
RED	Rot	4
MAGENTA	Magenta	5
YELLOW	Gelb	6
WHITE_NORMAL_INTENSITY	Weiß mit normaler Intensität	7
GRAY	Grau	8
LIGHT_BLUE	Hellblau	9
LIGHT_GREEN	Hellgrün	10
LIGHT_CYAN	Cyan (hell)	11
LIGHT_RED	Hellrot	12
LIGHT_MAGENTA	Magenta (hell)	13
BLACK	Schwarz	14
WHITE_HIGH_INTENSITY	Weiß mit hoher Intensität	15
BROWN	Braun	16
PINK	Rosa	17
TURQUOISE	Türkis	18

5.8.5 ControlKey

Das ControlKey-Objekt definiert Konstanten zum Senden von Cursor-Steuertasten und Hostbefehlen mithilfe der sendKeys-Methode. Konstanten sind für die folgenden Hosttypen verfügbar:

- IBM 3270
- IBM 5250
- VT
- UTS

IBM 3270

Schlüsselwort	Beschreibung
ALTVIEW	Alternative Ansicht
ATTN	Abruf
BACKSPACE	Rückschritt
BACKTAB	Rücktabulator
CLEAR	Löschen oder Bildschirminhalt löschen
CURSOR_SELECT	Cursorauswahl
DELETE_CHAR	Löschen, Zeichen löschen
DELETE_WORD	Wort löschen
DEST_BACK	Rückschritt mit Löschen
DEV_CANCEL	Geräteabbruch
DOWN	Cursor nach unten
DSPSOSI	SO/SI anzeigen
DUP	Feld duplizieren
END_FILE	Feldende
ENTER	Eingabe
ERASE_EOF	Feldende löschen
ERASE_FIELD	Feld löschen
ERASE_INPUT	Eingabe löschen
FIELD_MARK	Feldmarkierung
HOME	Cursor Pos1
IDENT	Ident
INSERT	Einfügen
LEFT_ARROW	Cursor nach links
LEFT2	Cursor um zwei Positionen nach links
NEW_LINE	Neue Zeile
PA1 – PA3	PA1 – PA3

Schlüsselwort	Beschreibung
PF1 – PF24	PF1 – PF24
PAGE_DOWN	Bild nach unten
PAGE_UP	Bild nach oben
RESET	Zurücksetzen, Terminal zurücksetzen
RIGHT2	Cursor um zwei Positionen nach rechts
RIGHT_ARROW	Cursor rechts, rechts
SYSTEM_REQUEST	Systemanforderung
TAB	Tabulatortaste
UP	Cursor nach oben

IBM 5250

Schlüsselwort	Beschreibung
ALTVIEW	Alternative Ansicht
ATTN	Abruf
AU1 – AU16	AU1 – AU16
BACKSPACE	Rückschritt
BACKTAB	Rücktabulator
BEGIN_FIELD	Feld beginnen
CLEAR	Löschen oder Bildschirminhalt löschen
DELETE_CHAR	Löschen, Zeichen löschen
DEST_BACK	Rückschritt mit Löschen
DOWN	Cursor nach unten
DSPSOSI	SO/SI anzeigen
DUP	Feld duplizieren
END_FILE	Feldende
ENTER	Eingabe
ERASE_EOF	Feldende löschen
ERASE_FIELD	Feld löschen
ERASE_INPUT	Eingabe löschen
FIELD_EXT	Feldende
FIELD_MINUS	Feld Minus
FIELD_PLUS	Feld Plus
FIELD_MARK	Feldmarkierung
HELP	Hilfeanforderung
HEXMODE	Hexadezimalmodus
HOME	Cursor Pos1
INSERT	Einfügen
LEFT_ARROW	Cursor nach links

Schlüsselwort	Beschreibung
NEW_LINE	Neue Zeile
PA1 – PA3	PA1 – PA3
PF1 – PF24	PF1 – PF24
PAGE_DOWN	Bild nach unten
PAGE_UP	Bild nach oben
[print]	Drucken
RESET	Zurücksetzen, Terminal zurücksetzen
RIGHT_ARROW	Cursor rechts, rechts
SYSTEM_REQUEST	Systemanforderung
TAB	Tabulatortaste
UP	Cursor nach oben

VT

Schlüsselwort	Beschreibung
BACKSPACE	Rückschritt
BREAK	Unterbrechungstaste
CLEAR	Löschen oder Bildschirminhalt löschen
CURSOR_SELECT	Cursorauswahl
DELETE_CHAR	Löschen, Zeichen löschen
DOWN	Cursor nach unten
EK_FIND	Nt Suche bearbeiten
EK_INSERT	Nt Einfügen bearbeiten
EK_NEXT	Nt Nächster bearbeiten
EK_PREV	Nt Vorheriger bearbeiten
EK_REMOVE	Nt Löschen bearbeiten
EK_SELECT	Nt Auswählen bearbeiten
END_FILE	Feldende
ENTER	Eingabe
F1 - F24	F1 - F24
HOLD	Halten
HOME	Pos1
INSERT	Einfügen
KEYPAD_COMMA	NtKomma
KEYPAD_DOT	NtDezimal
KEYPAD_ENTER	NtEingabe
KEYPAD_MINUS	NtMinus
KEYPAD0 - KEYPAD9	Nt0 - Nt9
LEFT_ARROW	Cursor nach links
PF1 - PF20	PF1 - PF20
PAGE_DOWN	Bild nach unten

Schlüsselwort	Beschreibung
PAGE_UP	Bild nach oben
RESET	Zurücksetzen, Terminal zurücksetzen
RETURN	Zurück, Wagenrücklauf
RIGHT_ARROW	Cursor rechts, rechts
TAB	Tabulatortaste
UDK16 – UDK20	Benutzertaste 6 – Benutzertaste 20
UP	Cursor nach oben

UTS

Schlüsselwort	Beschreibung
BACKSPACE	Rückschritt
BACKTAB	Rücktabulator
CHAR_ERASE	Löscht Zeichen an der Cursorposition und erweitert den Cursor.
CLEAR_DISPLAY	Bildschirminhalt löschen
CLEAR_EOD	Bis zum Anzeigeende löschen
CLEAR_EOF	Bis zum Feldende löschen
CLEAR_EOL	Bis zum Zeilenende löschen
CLEAR_FCC	Feldsteuerungszeichen löschen
CLEAR_HOME	Bildschirminhalt löschen und Cursor Pos1
CONTROL_PAGE	Blendet die Steuerungsseite ein oder aus
DELETE_LINE	Löscht die Zeile, in der sich der Cursor befindet, und verschiebt die restlichen Zeilen um eine Zeile nach oben.
DELIN_LINE	Löscht das Zeichen unterhalb des Cursors und verschiebt die restlichen Zeichen auf der Zeile nach links.
DELIN_PAGE	Löscht das Zeichen unterhalb des Cursors und verschiebt die restlichen Zeichen auf der Seite nach links.
DOWN	Verschiebt den Cursor um eine Zeile nach unten. Umbruch erfolgt am unteren Ende.
DUP_LINE	Erstellt eine Kopie der aktuellen Zeile und überschreibt die nächste Zeile mit dem Duplikat.
END_FIELD	Bewegt den Cursor an das Ende des aktuellen Felds.
END_PAGE	Bewegt den Cursor an das Ende der aktuellen Seite.
EURO	Fügt das Euro-Zeichen ein.
F1 - F22	Funktionstasten F1-F22
HOME	Bewegt den Cursor an den Anfang der aktuellen Seite (Zeile 1, Spalte 1)
INSERT	Wechselt zwischen dem Einfügemodus und dem Überschreibmodus.

Schlüsselwort	Beschreibung
INSERT_IN_LINE	Fügt ein Leerzeichen an der Cursorposition ein und verschiebt die restlichen Zeichen auf der Zeile nach rechts. Das Zeichen in der äußeren rechten Spalte der Zeile wird verworfen.
INSERT_IN_PAGE	Fügt ein Leerzeichen an der Cursorposition ein und verschiebt die restlichen Zeichen auf der Seite nach rechts. Das Zeichen in der äußeren rechten Spalte der jeweiligen Zeile wird verworfen.
INSERT_LINE	Fügt eine neue Zeile an der Cursorzeile ein und verschiebt die restlichen Zeilen nach unten. Die letzte Zeile auf der Seite wird verworfen.
LEFT_ARROW	Bewegt den Cursor um eine Position nach links und fügt ggf. einen Umbruch ein.
LOCATE_FCC	Sucht nach dem nächsten Feldsteuerungszeichen auf dem Bildschirm.
MSG_WAIT	Ruft Meldungen in der Warteschleife des Terminals ab.
RETURN	Wagenrücklauf
RIGHT_ARROW	Bewegt den Cursor um eine Position nach rechts und fügt ggf. einen Umbruch ein.
SOE	Fügt das Zeichen für den Anfang des Eintrags ein.
START_OF_FIELD	Bewegt den Cursor an den Feldanfang.
START_OF_LINE	Bewegt den Cursor zur ersten Spalte der aktuellen Zeile.
TAB	Bewegt den Cursor in die nächste Tabulatorposition auf dem Bildschirm.
TOGGLE_COL_SEP	Ändert das Spaltentrennzeichen-Attribut.
TOGGLE_STRIKE_THRU	Ändert das Durchstreichungs-Attribut in der aktuellen Datenzelle.
TOGGLE_UNDERLINE	Ändert das Unterstreichungs-Attribut in der aktuellen Datenzelle.
TRANSMIT	Überträgt die geänderten Felddaten an den Host.
UNLOCK	Sendet die UNLOCK-Taste an den Host.
UP	

Schlüsselwort	Beschreibung
	Bewegt den Cursor eine Zeile nach oben und fügt ggf. einen Umbruch ein.

5.8.6 DataCell

Das DataCell-Objekt stellt Informationen zu einer bestimmten Position auf einem Terminalbildschirm bereit.

Methode	Beschreibung
`getPosition()`	Gibt die Position dieser Datenzelle auf dem Bildschirm zurück. **Rückgabe** `{Position}` Position dieser Datenzelle auf dem Bildschirm.
`getChar()`	Ruft das mit der Zelle verknüpfte Zeichen ab. **Rückgabe** `{String}` Das mit der Zelle verknüpfte Zeichen.
`getAttributes()`	Gibt die für diese Datenzelleninstanz angegebene Attributgruppe zurück. Siehe AttributeSet. **Rückgabe** `{AttributeSet}` Attributsatz für diese Datenzelleninstanz.
`getForegroundColor()`	Gibt die Vordergrundfarbe für diese Datenzelle gemäß der Definition im Color-Objekt zurück. **Rückgabe** `{Number}` Vordergrundfarbe für diese Datenzelle. Die Farbe wird im Color-Objekt definiert.
`getBackgroundColor()`	Gibt die Hintergrundfarbe für diese Datenzelle gemäß der Definition im Color-Objekt zurück. **Rückgabe** `{Number}` Hintergrundfarbe für diese Datenzelle. Die Farbe wird im Color-Objekt definiert.
`toString`	Konvertiert die interne Datenzelle in eine Zeichenfolge. **Rückgabe** `{String}` Die Zeichenkettendarstellung einer Datenzelle.
`isFieldDelimiter()`	Testet, ob die Zelle ein Feldtrennzeichen darstellt. **Rückgabe** `{Boolean}` „True“ (wahr), wenn diese Zelle ein Feldtrennzeichen darstellt, ansonsten „False“ (falsch).

5.8.7 Dimension

Stellt die Größe des Bildschirms oder des Bildschirmbereichs dar.

Methode	Beschreibung
`Dimension(rows,cols)`	Erstellt eine neue Dimension-Instanz. **Parameter** `{Number} rows` Bildschirmzeilendimension `{Number} cols` Bildschirmspaltendimension

5.8.8 Field

Verwenden Sie das Field-Objekt gemeinsam mit FieldList, um die auf dem Bildschirm in einem Feld enthaltenen Informationen abzurufen.

Methode	Beschreibung
`getAttributes()`	Gibt die für diese Feldinstanz angegebene Attributgruppe zurück. Siehe AttributeSet. **Rückgabe** `{AttributeSet}` Der Attributsatz für dieses Feld.
`getForegroundColor()`	Gibt die Vordergrundfarbe des Felds zurück. **Rückgabe** `{Number}` Vordergrundfarbe für dieses Feld. Diese Werte werden im Color-Objekt definiert.
`getBackgroundColor()`	Gibt die Hintergrundfarbe des Felds zurück. **Rückgabe** `{Number}` Hintergrundfarbe für dieses Feld. Diese Werte werden im Color-Objekt definiert.
`getStart()`	Gibt die Anfangsposition des Felds zurück. Die Anfangsposition ist die Position des ersten Zeichens im Feld. Einige Hosttypen verwenden eine Zeichenposition zum Speichern von Feldebenenattributen. In diesem Fall wird die Attributposition nicht als Anfangsposition betrachtet. **Rückgabe** `{Position}` Anfangsposition des Felds. **Fehlerrückgabe** `{RangeError}` Für Felder mit einer Länge von null.
`getEnd()`	Gibt die Endposition des Felds zurück. Die Endposition ist die Position im Darstellungsbereich mit dem letzten Zeichen des Felds. **Rückgabe** `{Position}` Endposition des Felds. **Fehlerrückgabe** `{RangeError}` Für Felder mit einer Länge von null.
`getLength()`	Gibt die Länge des Felds zurück. Bei Hosttypen, die zum Speichern der Feldattribute eine Zeichenposition verwenden, ist die Feldattributposition nicht in der Feldlänge enthalten. **Rückgabe** `{Number}` Länge des Felds.
`getDataCells()`	Ruft die Datenzellen ab, die dieses Feld bilden. Siehe DataCell. **Rückgabe** `{DataCell[]}` Datenzellen, die dieses Feld bilden.

`getText()`	Ruft den Text aus dem Feld ab. **Rückgabe** `{String}` Feldtext.
`setText()`	Legt den Feldtext fest. Bei bestimmten Hosttypen wie VT wird der Text sofort an den Host übertragen. Bei anderen Hosttypen wiederum wird der Text erst dann an den Host übertragen, wenn die AID-Taste aufgerufen wird. Wenn der Text kürzer als das Feld ist, wird er im Hostfeld platziert, und der Rest des Felds wird gelöscht. Wenn der Text länger als das Hostfeld ist, wird so viel Text wie möglich im Feld platziert. **Parameter** `{String}` Text, der im Feld gesetzt wird. **Fehlerrückgabe** `{Error}` Wenn das Feld geschützt ist.
`clearField()`	Löscht das aktuelle Feld emulationsspezifisch. **Fehlerrückgabe** `{Error}` Wenn das Feld geschützt ist oder Löschen nicht unterstützt wird.
`getPresentationSpace()`	Ruft den PresentationSpace ab, der dieses Feld erstellt hat. **Rückgabe** `{PresentationSpace}` Übergeordnetes Element dieser Feldinstanz.
`toString()`	Erstellt eine benutzerfreundliche Beschreibung des Felds. **Rückgabe** `{String}` Eine von Benutzern lesbare Darstellung des Felds.

5.8.9 FieldList

Verwenden Sie das FieldList-Objekt gemeinsam mit dem Field-Objekt zum Abrufen von Feldlisteninformationen.

Methode	Beschreibung
`getPresentationSpace()`	Ruft den PresentationSpace ab, der dieses Feld erstellt hat. **Rückgabe** `{PresentationSpace}` Übergeordnetes Element dieser Feldinstanz.
`findField(position, text, direction)`	Gibt das Feld mit dem angegebenen Text zurück. Der Suchvorgang beginnt an der angegebenen Position und verläuft vorwärts oder rückwärts. Wenn sich die Zeichenfolge über mehrere Felder erstreckt, wird das Feld zurückgegeben, das die Startposition enthält. Wenn vorwärts gesucht wird, findet kein Umbruch bis zum oberen Ende des Bildschirms statt. Wenn rückwärts gesucht wird, findet kein Umbruch bis zum unteren Ende des Bildschirms statt. **Parameter** `{Position}` Position, an der die Suche beginnen soll. Siehe Objekt „Position“. `{String}` Der Text, nach dem gesucht werden soll (optional). Wenn nicht angegeben, wird das nächste Feld rechts von oder unterhalb der angegebenen Position zurückgegeben. `{Number}` Richtung der Suche (optional). Verwenden Sie PresentationSpace. SearchDirection-Konstanten für diesen Parameter. Zum Beispiel: PresentationSpace.SearchDirection.FORWARD oder PresentationSpace.SearchDirection.BACKWARD. Wenn nicht angegeben, wird vorwärts gesucht. **Rückgabe** `{Field}` Enthält die Zeichenkette oder Null, wenn kein Feld, das die vorgegebenen Kriterien erfüllt, gefunden wird. **Fehlerrückgabe** `{RangeError}` Wenn die Position außerhalb des Wertebereichs liegt.
`get(index)`	Ruft das Feld am vorgegebenen Index ab. **Parameter** `{Number}` Index in der Feldliste. **Rückgabe** `{Field}` Feld am angegebenen Index. **Fehlerrückgabe** `{RangeError}` Wenn der Index außerhalb des Wertebereichs liegt.

`isEmpty()`	Gibt an, ob die Feldliste leer ist. **Rückgabe** `{Boolean}` „True“ (wahr), wenn die Liste leer ist.
`size()`	Gibt die Anzahl der in der Liste enthaltenen Felder an. **Rückgabe** `{Number}` Die Feldanzahl.
`toString()`	Erstellt eine benutzerfreundliche Beschreibung der Feldliste. **Rückgabe** `{String}` Eine von Benutzern lesbare Darstellung der Feldliste.

5.8.10 FileTransfer

Verwenden Sie das FileTransfer-Objekt, um Dateien aufzulisten und zwischen dem Hostsystem und dem Client zu übertragen.

Die Dateiübertragungs-API von Host Access for the Cloud abstrahiert die in verschiedenen Hostdateiimplementierungen verwendeten Benennungskonventionen für Dateipfade. Verwenden Sie das Format für URL- oder Linux-Dateisystempfade, wenn Sie die von der API verwendeten Pfade formatieren. Beispiel: `/stamm/verzeichnis/datei`.

Alle spezifischen Regeln in den jeweiligen Hostsystemen müssen berücksichtigt werden, z. B. zulässige Zeichen oder Namenlängen.

Hinweis

Browser enthalten erhebliche Sicherheitseinschränkungen in Bezug auf die Möglichkeit der Interaktion zwischen JavaScript und Clientdateisystemen.

Methode	Beschreibung
`getHostFileListing(remotePath)()`	Fordert eine Liste der Hostdateien an. Wenn `remotePath` nicht angegeben ist, wird eine Dateiliste für das aktuelle Remotearbeitsverzeichnis angezeigt. **Parameter** `{String}` (optional) Wenn dieser Wert angegeben ist, wird die Dateiliste für den angegebenen Remotepfad abgerufen. Wenn kein Wert angegeben wird, wird die Dateiliste für das aktuelle Remotearbeitsverzeichnis abgerufen. **Rückgabe** `{Promise}` Wird in ein Array von HostFile-Objekten aufgelöst, die in remoteName enthalten sind. Wird abgelehnt, wenn der Remotepfad nicht gelesen werden kann.
`sendFile(localFile, remoteName)`	Sendet die angegebene Datei an den Host. **Parameter** `{File}` JavaScript-Dateiobjekt, das auf die zu sendende lokale Datei verweist. `{String}` (optional) Vollständiger Remotedateiname entsprechend der Zulässigkeit im Remotesystem (Unix, Windows, MVS, VAX). **Rückgabe** `{Promise}` Wird mit einem `HostFile`-Objekt erfüllt, das die erfolgreich gesendete Datei darstellt. Wird abgelehnt, wenn beim Senden der Datei ein Fehler aufgetreten ist.
`getDownloadURL(remoteName)`	Erstellt einen Link zum Herunterladen einer Datei von einem Hostsystem. **Parameter** `{String}` Vollständiger Remotedateiname entsprechend der Zulässigkeit im Remotesystem (Unix, Windows, MVS, VAX). **Rückgabe** `{URL}` URL, die zum Abrufen der Datei vom Host Access for the Cloud-Sitzungsserver verwendet werden kann.
`setTransferOptions(options)`	Legt Übertragungsoptionen für die aktuelle FileTransfer-Sitzung fest. Die

	Übertragungsoptionen werden auf alle zukünftigen Übertragungen angewendet, bis die Sitzung entweder beendet oder durch einen anderen Aufruf von `setTransferOptions` überschrieben wird. **Parameter** `{JSON}` Siehe FileTransferOptions für zulässige Namen und Werte. **Rückgabe** `{Promise}` Wird erfüllt, wenn der Aufruf abgeschlossen wird. Wird abgelehnt, wenn beim Festlegen der Optionen ein Fehler aufgetreten ist.
`cancel()`	Bricht die aktuelle laufende Übertragung ab. **Parameter** `{String}` Vollständiger Remotedateiname entsprechend der Zulässigkeit im Remotesystem (Unix, Windows, MVS, VAX). **Rückgabe** `{Promise}` Wird erfüllt, wenn der Aufruf abgeschlossen wird. Wird abgelehnt, wenn während des Abbruchs der Übertragung ein Fehler aufgetreten ist.

5.8.11 FileTransferFactory

Ein fileTransferFactory-Objekt ist für alle Makros verfügbar. Wenn Dateiübertragungen für die Sitzung konfiguriert sind, können Sie mithilfe dieses Objekts einen Verweis auf ein FileTransfer-Objekt abrufen.

Methode	Beschreibung
`getIND$File()`	Gibt ein FileTransfer-Objekt für die Interaktion mit dem konfigurierten Ind$File-Typ für die Sitzung zurück. **Rückgabe** `{FileTransfer}` **Fehlerrückgabe** `{Error}` Wenn die Sitzung nicht für IND$File-Übertragungen konfiguriert wurde.

5.8.12 FileTransferOptions

Spezifikation des FileTransferOptions-Objekts. Beispiel:
`fileTransfer.setTransferOptions({ transferMethod : 'ascii' });```

Methode	Beschreibung
`transferMethod`	`{String}` Zulässige Werte: • ‘ascii’ • ‘Binär’

5.8.13 HostFile

Ein HostFile-Objekt stellt eine Datei auf dem Hostdateisystem dar.

Methode	Beschreibung
`getName()`	Ruft den Dateinamen ab.. **Rückgabe** `{String}` Der Dateiname.
`getParent()`	Ruft das übergeordnete Element dieser Hostdatei ab.. **Rückgabe** `{String}` Übergeordnetes Element dieser Hostdatei. Je nach Hosttyp handelt es sich dabei um ein unterschiedliches Element. Auf einem TSO-Host ist dies beispielsweise der Name des Katalogs, in dem sich die Datei befindet.
`getSize()`	Die Bytegröße der Datei.. **Rückgabe** `{Number}` Die Größe der Datei in Byte.
`getType()`	Der Typ der dargestellten Datei.. **Rückgabe**

5.8.14 HostFileType

Das HostFileType-Objekt definiert Konstanten zum Festlegen des Typs eines HostFile-Objekts.

Value (Wert)	Description (Beschreibung)
FILE	Stellt eine Datei auf dem Hostsystem dar.
DIR	Stellt ein Verzeichnis auf dem Hostsystem dar.
UNKNOWN	Stellt eine Hostdatei unbekannten Ursprungs dar.

5.8.15 OIA

Operatorinformationsfeld-Oberfläche (OIA, Operator Information Area). Das OIA-Objekt gibt Werte zurück, die im OIAStatus-Objekt definiert sind.

Methode	Beschreibung
`getStatus ()`	Gibt den Satz der aktivierten Statusflaggen zurück. Siehe StatusSet. **Rückgabe** `{StatusSet}` Statussatz, der die Statusinformationen enthält.
`getCommErrorCode()`	Gibt den Fehlercode zur aktuellen Kommunikation zurück. **Rückgabe** `{Number}` Code des aktuellen Kommunikationsfehlers. Wenn kein Fehlercode vorhanden ist, lautet der Wert 0.
`getProgErrorCode()`	Gibt den Fehlercode zum aktuellen Programm zurück.. **Rückgabe** `{Number}` Code des aktuellen Programmfehlers. Wenn kein Fehlercode vorhanden ist, lautet der Wert 0.

5.8.16 OIAStatus

OIAStatus	Beschreibung
CONTROLLER_READY	Controller bereit
A_ONLINE	Online mit einer Nicht-SNA-Verbindung
MY_JOB	Verbunden mit einer Hostanwendung
OP_SYS	Verbunden mit einer SSCP-Verbindung (SNA)
UNOWNED	Nicht angeschlossen
TIME	Tastatur gesperrt
SYS_LOCK	Systemsperre nach AID-Taste
COMM_CHECK	Kommunikationsprüfung
PROG_CHECK	Programmprüfung
ELSEWHERE	Tastenfolge an Cursorposition ungültig
FN_MINUS	Funktion nicht verfügbar
WHAT_KEY	Tastenfolge ungültig
MORE_THAN	Zu viele Zeichen wurden im Feld eingegeben
SYM_MINUS	Eingegebenes Symbol nicht verfügbar
INPUT_ERROR	Operator-Eingabefehler (nur 5250)
DO_NOT_ENTER	Nicht eingeben
INSERT	Cursor im Einfügemodus
GR_CURSOR	Cursor im Grafikmodus
COMM_ERR_REM	Erinnerung Kommunikationsfehler
MSG_WAITING	Anzeige für Nachricht vorhanden
ENCRYPT	Sitzung ist verschlüsselt
NUM_FIELD	Ungültiges Zeichen in einem Feld für numerische Daten

5.8.17 Position

Methode	Beschreibung
`Position(row,col)`	Erstellt eine neue Position-Instanz. **Parameter** `{Number} row` Koordinate der Bildschirmzeile. `{Number} col` Koordinate der Bildschirmspalte.

5.8.18 PresentationSpace

Verwenden Sie das PresentationSpace-Objekt zur Interaktion mit dem Terminalbildschirm. Zu den verfügbaren Interaktionen zählen das Einrichten und Abrufen der Cursorposition, das Senden von Tasten und das Lesen von Text.

Methode	Beschreibung
`getCursorPosition()`	Gibt eine Position-Instanz zurück, die die aktuelle Cursorposition darstellt. Eine Sitzung ohne Verbindung hat die Cursorposition 0,0. **Rückgabe** `{Position}` Aktuelle Cursorposition.
`setCursorPosition(position)`	Bewegt den Hostcursor an die angegebene Zeilen- und Spaltenposition. Bei einigen Hosts wie VT werden die Cursorbewegungen durch den Host eingeschränkt. **Parameter** `{Position}` Position Neue Cursorposition. **Rückgabe** Keine. **Fehlerrückgabe** `{RangeError}` Wenn die Position auf dem aktuellen Bildschirm nicht gültig ist.
`isCursorVisible()`	Testet, ob der Cursor aktuell im Präsentationsbereich angezeigt wird. Wenn die Sitzung nicht verbunden ist, wird der Cursor als nicht sichtbar betrachtet. **Rückgabe** `{Boolean}` „True“ (wahr), wenn der Cursor sichtbar ist. 'False', wenn der Cursor nicht angezeigt wird.
`sendKeys(keys)`	Überträgt eine Textzeichenkette oder ControlKey an der aktuellen Cursorposition im Präsentationsbereich an den Host. Wenn sich der Cursor nicht an der gewünschten Position befindet, verwenden Sie zunächst die `setCursorPosition`-Funktion. Die Textzeichenkette kann eine beliebige Anzahl an Zeichen und ControlKey-Objekten enthalten. Ein Beispiel: "meinname" + `ControlKey.TAB` + "meinpass" + `ControlKey.ENTER` überträgt eine Benutzer-ID, tabuliert zum nächsten Feld, überträgt ein Passwort und sendet dann die Eingabetaste. Um eine eckige Klammer zu übertragen, geben Sie die Klammern doppelt ein ([[oder]]). **Parameter** `{String} keys` Text und/oder Steuertasten, der/die übertragen werden soll(en).
`getText(start,length)`	Gibt eine Zeichenfolge zurück, die einen linearen Bereich des Präsentationsbereichs darstellt. Wenn

	Zeilengrenzen auftreten, werden keine Zeichen für neue Zeilen eingefügt. **Parameter** `{Position} start` Position, ab der Text abgerufen werden soll. `{Number} length` Maximale Anzahl an Zeichen, die zurückgegeben werden sollen. Wenn durch den Längenparameter (length) die letzte Position des Präsentationsbereichs überschritten wird, werden nur die Zeichen bis zur letzten Position zurückgegeben. **Rückgabe** `{String}` Zeichenkette, die einen linearen Bereich des Präsentationsbereichs darstellt, der leer sein kann, wenn die Sitzung nicht verbunden ist. **Fehlerrückgabe** `{RangeError}` Wenn die Position oder Länge auf dem aktuellen Bildschirm ungültig ist.
`getSize()`	Ruft die Abmessungen des Bildschirms als Dimension-Objekt ab. **Rückgabe** `{Dimension}` Enthält die Anzahl an Zeilen und Spalten. Die Bildschirmgröße beträgt [row:0, col:0], wenn die Sitzung nicht verbunden ist.
`getDataCells(start, length)`	Gibt DataCell-Instanzen zurück, bei denen das erste Mitglied für die durch den Startparameter angegebene Position gedacht ist. Die maximale Anzahl an DataCell-Instanzen in der Liste wird durch den Längenparameter angegeben. **Parameter** `{Position} start` Die erste Position auf dem Hostbildschirm, auf dem DataCell-Instanzen abgerufen werden sollen. Siehe Position. `{Number} length` Maximale Anzahl an DataCell-Instanzen, die abgerufen werden sollen. Wenn die Länge nicht angegeben ist, werden DataCell-Instanzen von der Startposition bis zum Ende des Bildschirms zurückgegeben. **Rückgabe** `{DataCell[]}` Instanzen, die leer sein können, wenn die Sitzung nicht verbunden ist. Wenn die Position nicht angegeben ist, werden alle DataCell-Instanzen zurückgegeben. Wenn die Länge nicht angegeben ist,

	werden DataCell-Instanzen von der Startposition bis zum Ende des Bildschirms zurückgegeben. **Fehlerrückgabe** `{RangeError}` Wenn „start“ oder „length“ außerhalb des Wertebereichs liegt.
`getFields()`	Gibt eine Liste der Felder im Präsentationsbereich zurück. Wenn der Hosttyp keine Felder unterstützt oder der aktuelle Bildschirm nicht formatiert wurde, ist der Rückgabewert immer eine leere Liste. Siehe FieldList. **Rückgabe** `{FieldList}` Liste der vom Host definierten Felder im Präsentationsbereich.

5.8.19 Session

Bei dem Session-Objekt handelt es sich um den Hauptzugriffspunkt für die Interaktion mit dem Host. Es enthält Funktionen zum Herstellen und Trennen einer Verbindung und zum Abrufen des PresentationSpace-Objekts.

Methode	Beschreibung
`connect()`	Stellt die Verbindung zum konfigurierten Host her. Verwenden Sie ggf. `wait.forConnect()`, um die Makroausführung zu blockieren, bis die Verbindung hergestellt wurde. **Rückgabe** `Keine`
`disconnect()`	Trennt die Sitzung zum konfigurierten Host. Verwenden Sie ggf. `wait.forDisconnect()`, um die Makroausführung zu blockieren, bis die Verbindung hergestellt wurde. **Rückgabe** `Keine`
`isConnected()`	Gibt an, ob eine Verbindung zum Host besteht. **Rückgabe** `{Boolean}` „True“ (wahr), wenn die Hostverbindung hergestellt wurde, „False“ (falsch), wenn keine Verbindung hergestellt wurde.
`getPresentationSpace()`	Gewährt Zugriff auf die PresentationSpace-Instanz für diese Sitzung. **Rückgabe** `{PresentationSpace}` Instanz, die dieser Sitzung zugeordnet ist.
`getDeviceName()`	Gibt für eine verbundene Sitzung den Gerätenamen zurück und gibt für eine getrennte Sitzung oder Sitzung ohne Gerätenamen eine leere Zeichenkette zurück. **Rückgabe** `{String}` Der Name des verbundenen Geräts.
`getType()`	Gibt den Typ der Hostsitzung zurück. Weitere Informationen finden Sie unter SessionType. **Rückgabe** `{String}` Der Typ der Hostsitzung.
`setDeviceName()`	Bietet eine Möglichkeit, in einer Sitzungsinstanz den Gerätenamen zu ändern. **Parameter** `{String} name` Gerätename, der bei der Herstellung einer Verbindung zu einem Host verwendet werden soll. **Fehlerrückgabe**

	`{Error}` Wenn während einer hergestellten Sitzung versucht wurde, den Gerätenamen festzulegen.
`getOIA()`	Bietet Zugriff auf die OIA-Instanz für diese Sitzung. **Rückgabe** `{OIA}` Mit dieser Sitzung verknüpfte OIA-Instanz.

5.8.20 SessionType

Konstanten zum Identifizieren des Hosttyps, zu dem die Verbindung hergestellt wird. Siehe Session-Objekt.

Hosttyp	Beschreibung
IBM_3270	IBM 3270-Terminalsitzung
IBM_5250	IBM 5250-Terminalsitzung
VT	VT-Sitzung

5.8.21 StatusSet

Mit dem StatusSet-Objekt können Sie den Status des OIA-Objekts decodieren. Das StatusSet-Objekt gibt die im OIAStatus-Objekt definierten Werte zurück. Wenn sie gemeinsam verwendet werden, können Sie die Statusinformationen aus dem OIA-Objekt abrufen.

Methode	Beschreibung
`contains(statusFlag)`	Ermittelt, ob der Satz die angegebene Statusflagge aus OIAStatus-Konstanten enthält. **Parameter** `{Number} statusFlag` Zu überprüfender Status. **Rückgabe** `{Boolean}` „True“ (wahr), wenn die Statusflagge im Satz vorhanden ist.
`isEmpty()`	Gibt an, ob der Statussatz leer ist. **Rückgabe** `{Boolean}` „True“ (wahr), wenn der Satz leer ist.
`size()`	Gibt die Anzahl der in dem Satz enthaltenen Statuskennzeichen an. **Rückgabe** `{Number}` Die Statusanzahl.
`toArray()`	Konvertiert den internen Statussatz in ein Array. **Rückgabe** `{Object []}` Array mit den Statusflaggen im Satz.
`toString()`	Konvertiert den internen Statussatz in eine Zeichenfolge. **Rückgabe** `{String}` Durch Leerzeichen getrennte Namen der im Satz enthaltenen Statusflaggen.
`forEach(callback, thisArg)`	Funktion zum Durchlaufen der einzelnen Elemente im Statussatz. **Parameter** `{forEachCallback}` Callback zum Ausführen eines bestimmten Vorgangs. Wird gemeinsam mit dem Namen des jeweiligen Status im Satz aufgerufen.
`forEachCallback(string, thisArg)`	Eine durch Benutzer bereitgestellte Callback-Funktion, mit der Sie das Verhalten bereitstellen. Wird als Callback-Parameter für „forEach“ verwendet. **Parameter** `{String} string` Der Name eines Status im Statussatz. `{Object} thisArg` Optionaler Verweis auf ein Kontextobjekt.

5.8.22 User Interface

Das UI-Objekt stellt Funktionen zur Interaktion mit dem Benutzer sowie zur Abfrage und Anzeige von grundlegenden Informationen bereit. Das UI-Objekt ist in Ihrem Makro automatisch als ui-Variable verfügbar.

> **Hinweis**
>
> **Wichtig:** Allen UI-Funktionen muss das yield-Schlüsselwort voranstehen. Dadurch kann das Makro die Ausführung blockieren, bis die Bedingungen der UI-Funktion erfüllt wurden. `[parameter]` kennzeichnet einen optionalen Parameter.

Methode	Beschreibung
`prompt(message, [defaultAnswer], [mask])`	Fordert den Benutzer zur Eingabe von Informationen in der Benutzeroberfläche auf. **Parameter** `{String} message` Titel, der dem Benutzer angezeigt werden soll. Standard: leere Zeichenkette. `{String} defaultAnswer` Standardantwort, die verwendet werden soll, wenn der Benutzer keine andere Zeichenkette angibt. Standard: leere Zeichenkette. `{Boolean} mask` Gibt an, ob die Eingabeaufforderung ausgeblendet werden soll (wie bei einem Passwort). **Rückgabe** `{Promise}` Erfüllt, wenn der Benutzer das Dialogfeld schließt. Bei „OK“ wird eine Benutzereingabe zurückgegeben, „Abbrechen“ ergibt Null.

`message([message])`	Zeigt eine Meldung auf der Benutzeroberfläche an.
	Parameter
	`{String} message Meldung, die dem Benutzer angezeigt werden soll. Standard: leere Zeichenkette.`
	Rückgabe
	`{Promise} Erfüllt, wenn der Benutzer das Meldungsfenster schließt.`

5.8.23 Wait

Verwenden Sie das wait-Objekt, um auf einen bestimmten Sitzungs- oder Bildschirmstatus zu warten. Sie können beispielsweise darauf warten, dass der Cursor an einer bestimmten Position gefunden wird oder Text an einer bestimmten Position vorhanden ist, bevor Sie mit dem Ausführen des Makros fortfahren.

Wait-Funktionen werden häufig zusammen mit asynchronen Funktionen wie connect() oder sendKeys() verwendet.

Hinweis

Alle Funktionen unterstützen Timeoutwerte als optionale Parameter und verwenden einen standardmäßigen Timeoutwert von 10 Sekunden (10000 ms).
Wichtig: Allen wait-Funktionen muss das yield-Schlüsselwort voranstehen. Dadurch kann das Makro die Ausführung blockieren, bis die Bedingungen der wait-Funktion erfüllt wurden.
`[parameter]` kennzeichnet einen optionalen Parameter.

Methode	Beschreibung
`setDefaultTimeout(timeout)`	Legt den standardmäßigen Timeoutwert für alle Funktionen fest. **Parameter** `{Number}` Standardmäßiger Timeoutwert für alle wait-Funktionen in Millisekunden. **Rückgabe** `{None}` **Fehlerrückgabe** `{RangeError}` Wenn der angegebene Timeoutwert kleiner als null ist.
`forConnect([timeout])`	Wartet auf das Abschließen einer Verbindungsanforderung. **Parameter** `{Number}` In Millisekunden. **Rückgabe** `{Promise}` Erfüllt, wenn die Sitzung bereits verbunden wurde oder die Verbindung zustande kommt. Wird abgelehnt, wenn die Wartezeit überschritten wurde.
`forDisconnect([timeout])`	Wartet auf das Abschließen einer Anforderung zur Trennung einer Verbindung. **Parameter** `{Number}` Timeout in Millisekunden. **Rückgabe** `{Promise}` Erfüllt, wenn die Verbindung der Sitzung bereits getrennt wurde oder endgültig getrennt wird. Wird abgelehnt, wenn die Wartezeit überschritten wurde.
`forFixedTime([timeout])`	Wartet ohne Bedingungen für eine festgelegte Zeit. Die Zeit wird in Millisekunden (ms) angegeben.. **Parameter** `{Number}` Timeout in Millisekunden. **Rückgabe** `{Promise}` Nach dem Verstreichen der Zeit erfüllt.
`forScreenChange([timeout])`	Wartet auf eine Änderung des Hostbildschirms. Diese Funktion gibt eine Rückmeldung, wenn eine Bildschirmaktualisierung erkannt wird. Sie bietet keine Informationen über die Anzahl nachfolgender Aktualisierungen, die möglicherweise bis zur

	vollständigen Aktualisierung des Bildschirms erfolgen. Es empfiehlt sich, wiederholt zu warten, bis der Bildschirminhalt mit einem bekannten Endkriterium übereinstimmt.) **Parameter** `{Number}` Timeout in Millisekunden. **Rückgabe** `{Promise}` Erfüllt, wenn der Bildschirm geändert wurde. Wird abgelehnt, wenn die Wartezeit überschritten wurde.
`forCursor(position, [timeout])`	Wartet darauf, dass der Cursor die angegebene Position erreicht. **Parameter** `{Position}` Gibt die Zeile und Spalte an. **Rückgabe** `{Promise}` Erfüllt, wenn sich der Cursor bereits an der angegebenen Stelle befindet oder wenn er endgültig dort positioniert ist. Abgelehnt, wenn das Timeout überschritten wurde.
`forText(text, position, [timeout])`	Wartet auf Text an einer bestimmten Position auf dem Bildschirm. **Parameter** `{String}` Zu erwartender Text. `{Position}` Gibt die Zeile und Spalte an. `{Number}` Timeout in Millisekunden. **Rückgabe** `{Promise}` Erfüllt, wenn der Text bereits an der angegebenen Position ist oder sobald er dort positioniert ist. Abgelehnt, wenn das Timeout überschritten wurde. **Fehlerrückgabe** `{RangeError}` Wenn die Position ungültig ist.
`forHostPrompt(text, column, [timeout])`	Wartet auf eine Eingabeaufforderung in einer bestimmten Spalte auf dem Bildschirm. **Parameter** `{String}` Zu erwartende Textaufforderung. `{Number}` Spalte, in der der Cursor erwartet wird. `{Number}` Timeout in Millisekunden. **Rückgabe** `{Promise}` Erfüllt, wenn die Bedingungen bereits erfüllt sind oder nachdem sie endgültig erfüllt werden.

	Abgelehnt, wenn das Timeout überschritten wurde. **Fehlerrückgabe** `{RangeError}` Wenn die Spalte außerhalb des Wertebereichs liegt.
`forHostSettle([settleTime], [timeout])`	**HINWEIS:** `wait.forHostSettle` sollte nur verwendet werden, wenn andere gezieltere Wartefunktionen nicht ausreichen. Überwacht eingehende Bildschirmdaten und löst „settleTime ms“ nach der letzten Aktualisierung **und** Entsperren der Tastatur auf. Diese Funktion ist nützlich, wenn Daten in mehreren Paketen ankommen und Sie sicher sein möchten, dass der gesamte Bildschirm empfangen wurde, bevor Sie fortfahren. **Parameter** `{Number}` Zeit, für die nach der letzten Aktualisierung gewartet werden soll, um sicherzustellen, dass weitere Daten nicht unerwartet ankommen. Der Standardwert ist 200 Millisekunden. `{Number}` Timeout in Millisekunden. **Rückgabe** `{Promise}` Erfüllt, wenn die Wartezeit nach Erhalt der letzten Bildschirmaktualisierung verstrichen ist und die Tastatur entsperrt ist.

5.9 Beispielmakros

Die nachstehenden Beispiele eignen sich als Ausgangspunkt für die Erstellung erfolgreicher Makros, in denen die Funktionen des Makroeditors ideal genutzt werden.

5.9.1 Grundlegende Hostinteraktion

In diesem Beispiel wird die grundlegende Hostinteraktion dargestellt. Dazu zählen die folgenden Interaktionen:

- Daten an den Host senden
- Auf die Anzeige von Bildschirmen warten
- Das `yield`-Schlüsselwort verwenden, um auf asynchrone Funktionen zu warten
- Text auf dem Bildschirm lesen
- Dem Benutzer grundlegende Informationen anzeigen
- Fehlergrundlagen behandeln

Für alle Makros sind standardmäßig die folgenden Objekte verfügbar:

1. **session** – Haupteinstiegspunkt zum Host. Kann Verbindungen herstellen und trennen und bietet Zugriff auf das PresentationSpace-Objekt.

   Das aus der Sitzung abgerufene PresentationSpace-Objekt stellt den Bildschirm dar und bietet zahlreiche allgemeine Funktionen wie das Abrufen und Einrichten der Cursorposition, das Senden von Daten an den Host und das Lesen auf dem Bildschirm.

2. **wait** – Dieses Objekt bietet eine einfache Möglichkeit, auf das Auftreten der verschiedenen Hoststatus zu warten, bevor weitere Daten gesendet oder auf dem Bildschirm gelesen werden.

3. **UI** – Stellt die grundlegenden Funktionen der Benutzeroberfläche bereit. Zeigt Benutzern Daten an oder fragt Informationen von Benutzern ab.

```
// Neue Makrofunktion erstellen
var macro = createMacro(function*(){
'use strict';

// Für alle Makros sind standardmäßig die folgenden Objekte verfügbar:
// 1. session – Hauptzugriffspunkt zum Host. Kann Verbindungen herstellen und trennen und bietet
Zugriff auf das PresentationSpace-Objekt.
//    Das aus der Sitzung abgerufene PresentationSpace-Objekt stellt den Bildschirm dar und bietet
zahlreiche allgemeine Funktionen wie das Abrufen und Einrichten der
//    Cursorposition, das Senden von Daten an den Host und das Lesen auf dem Bildschirm.
// 2. wait - Dieses Objekt bietet eine einfache Möglichkeit, auf das Auftreten der verschiedenen
Hoststatus zu warten, bevor weitere Daten gesendet oder auf dem Bildschirm gelesen werden.
// 3. ui – Stellt die grundlegenden Funktionen der Benutzeroberfläche bereit. Benutzern Daten
anzeigen oder Informationen von Benutzern abfragen.

// Eine Variable zum Lesen und Anzeigen von Bildschirmdaten deklarieren.
// Es wird empfohlen, alle Variablen im oberen Bereich einer Funktion zu deklarieren.
var numberOfAccounts = 0;

// Mit dem Abrufen des PresentationSpace-Objekts beginnen, das zahlreiche gängige
Bildschirmoperationen bereitstellt.
var ps = session.getPresentationSpace();

try {
    // Kann die Cursorposition einrichten und abrufen
    ps.setCursorPosition(new Position(24, 2));

    // Die sendKeys-Funktion zum Senden von Zeichen an den Host verwenden
    ps.sendKeys('cics');

    // SendKeys wird auch zum Senden von Hosttasten wie PA- und PF-Tasten verwendet.
    // Siehe "Steuertasten" in der Dokumentation für alle verfügbaren Optionen
    ps.sendKeys(ControlKey.ENTER);

    // Darauf warten, dass der Cursor die korrekte Position erreicht.
    // Das wait-Objekt bietet verschiedene Funktionen zum Warten auf das Eintreten bestimmter
Status,
    // sodass Sie weitere Tasten senden oder Daten auf dem Bildschirm lesen können.
    yield wait.forCursor(new Position(24, 2));

    // Sie können Zeichen und Steuerungstasten gemeinsam in einem sendKeys-Aufruf verwenden.
    ps.sendKeys('data' + ControlKey.TAB + ControlKey.TAB + 'more data' + ControlKey.ENTER);

    // Das "yield"-Schlüsselwort muss allen "wait"- und "ui"-Funktionsaufrufen voranstehen.
    // Es weist den Browser an, die Ausführung des Makros anzuhalten, bis die
    // (asynchrone) wait-Funktion zurückgegeben wird. Informationen darüber, welche Funktionen das
yield-Passwort
    // erfordern, finden Sie in der Dokumentation.
    yield wait.forCursor(new Position(10, 26));
    ps.sendKeys('accounts' + ControlKey.ENTER);

    // Kann auch darauf warten, dass in bestimmten Bereichen des Bildschirms Text angezeigt wird
    yield wait.forText('ACCOUNTS', new Position(3, 36)) ;
    ps.sendKeys('1' + ControlKey.ENTER);
```

```
    // Alle wait-Funktionen werden unterbrochen, wenn die Kriterien nicht innerhalb einer
bestimmten Zeitspanne erfüllt werden.
    // Kann mit einem optionalen Parameter in den wait-Funktionen die Wartezeit erhöhen (in
Millisekunden)
    // Alle Wartezeiten werden in Millisekunden angegeben. Der Standardwert ist 10 Sekunden (10000
ms).
    yield wait.forCursor(new Position(1, 1), 15000);
    ps.sendKeys('A' + ControlKey.ENTER);

    // PS provides the getText function for reading text from the screen
    numberOfAccounts = ps.getText(new Position(12, 3), 5);

    // Use the ui object to display some data from the screen
    ui.message('Number of active accounts: ' + numberOfAccounts);

    // The try / catch allows all errors to be caught and reported in a central location
} catch (error) {
    // Again we use the ui object to display a message that an error occurred
    yield ui.message('Error: ' + error.message);
}
//End Generated Macro
});

// Run the macro and return the results to the Macro Runner
// The return statement is required as the application leverages
// this to know if the macro succeeded and when it is finished
return macro();
```

5.9.2 Benutzerinteraktion

Dieses Beispiel zeigt, wie Benutzer mithilfe der bereitgestellten API-Methoden zur Eingabe aufgefordert oder über eine Meldung benachrichtigt werden.

```
var macro = createMacro(function*(){
  'use strict';

  // Das "ui"-Objekt stellt Funktionen zur Abfrage und Anzeige von Informationen bereit

  // Variablen für eine spätere Verwendung deklarieren
  var username;
  var password;
  var flavor;
  var scoops;

  //Start generiertes Makro
  var ps = session.getPresentationSpace();

  try {
    // Benutzer zur Eingabe ihres Namens auffordern und den Namen in einer Variable speichern.
    // Das 'yield'-Schlüsselwort ist zum Blockieren der Ausführung erforderlich, während auf die Benutzereingabe gewartet wird.
    username = yield ui.prompt('Geben Sie Ihren Benutzernamen ein');

    // Benutzer mit bereitgestelltem Standard zur Eingabe eines Werts auffordern.
    flavor = yield ui.prompt('Was ist Ihre Lieblingseissorte?', 'Schokolade');

    // Benutzer über die 'mask'-Option zur Eingabe persönlicher Informationen auffordern. Das Eingabefeld wird bei der Eingabe maskiert.
    // Wenn ein Parameter nicht verwendet wird, kann mit 'null' angegeben werden, dass er nicht verwendet werden soll.
    // Hier zeigen wir durch die Angabe, dass wir keinen Standardwert zeigen müssen.
    password = yield ui.prompt('Geben Sie Ihr Passwort ein', null, true);

    // Die Aufforderung gibt null zurück, wenn der Benutzer nicht auf die Schaltfläche 'OK' klickt, sondern auf 'Abbrechen'.
    // Eine Möglichkeit zum Behandeln dieses Falls ist das Umbrechen des Aufrufs in einem try/catch-Block.
    scoops = yield ui.prompt('Wie viele Kugeln möchten Sie?');
    if (scoops === null) {
      // Dadurch wird das Makro beendet.
      return;
      // Alternativ könnte ein Fehler ausgegeben und im nachstehenden "Catch" erfasst werden
     }
     // Die gesammelten Werte verwenden, um das Eis zu bestellen
    ps.sendKeys(username + ControlKey.TAB + password + ControlKey.ENTER);
    yield wait.forCursor(new Position(5, 1));
    ps.sendKeys(flavor + ControlKey.TAB + scoops + ControlKey.ENTER);

     // Dem Benutzer eine Meldung anzeigen. Durch die Verwendung des 'yield'-Schlüsselworts vor dem Aufruf wird die
     // weitere Ausführung des Makros blockiert, bis der Benutzer auf die Schaltfläche 'OK' klickt.
    yield ui.message('Bestellung erfolgreich. Genießen Sie Ihr ' + scoops + ' Kugeln ' + flavor + ' Eiscreme ' + username + '!');
    } catch (error) {
     // Hier verwenden wir das ui-Objekt zum Anzeigen einer Fehlermeldung
    yield ui.message(error.message);
    }
    //Ende generiertes Makro
```

```
});

return macro();
```

5.9.3 Durchlaufen von Daten

Dieses Beispiel zeigt, wie eine beliebige Anzahl an Bildschirmen durchlaufen wird und die Daten auf den jeweiligen Bildschirmen verarbeitet werden.

```
// Neue Makrofunktion erstellen.
var macro = createMacro(function*(){
  'use strict';

  // Variable(n) für eine spätere Verwendung erstellen var password;
  var accountNumber;
  var transactionCount = 0;
  var row = 0;

  // Eine Referenz zum PresentationSpace-Objekt abrufen.
  var ps = session.getPresentationSpace();

  try {
    // Für die Anmeldung bei der Anwendung Benutzername und Passwort eingeben.
    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);

    // Anwendungsbefehl eingeben.
    yield wait.forCursor(new Position(20, 38));
    ps.sendKeys('4');
    ps.sendKeys(ControlKey.ENTER);

    // Transaktionen für ein Konto werden aufgelistet.
    yield wait.forCursor(new Position(13, 25));
    ps.sendKeys('2');
    // Kontonummer eingeben. Hier zur Erleichterung hartcodiert.
    yield wait.forCursor(new Position(15, 25));
    accountNumber = yield ui.prompt('Kontonummer:', '167439459');
    ps.sendKeys(accountNumber);
    ps.sendKeys(ControlKey.ENTER);

    // Warten, bis auf dem Kontoprofilbildschirm vorhanden
    yield wait.forText('ACCOUNT PROFILE', new Position(3, 33));

    // Nach Text suchen, der anzeigt, dass die letzte Seite des Datensatzes erreicht wurde
    while (ps.getText(new Position(22, 12), 9) !== 'LAST PAGE') {

      // Während die letzte Seite mit Datensätzen nicht erreicht wurde, zur nächsten Seite mit Datensätzen wechseln.
      ps.sendKeys(ControlKey.PF2);
      yield wait.forCursor(new Position(1, 1));

      // Wenn die Cursorposition nicht zwischen Datensatzbildschirmen wechselt und der Bildschirm keinen Text enthält,
      // können Sie prüfen, ob ein Bildschirm aktualisiert wurde. Sie können eine
      // festgelegte Zeitspanne warten, bis eine aid-Taste für den Aufbau des Bildschirms gesendet wird.
      // Zum Beispiel:
      // yield wait.forFixedTime(1000);

      // Für alle Zeilen die Zählvariable erhöhen, wenn sie Daten enthalten.
      for (row = 5; row <= 21; row++) {

        // Es befinden sich zwei Spalten auf dem Bildschirm. Daten in Spalte 1 prüfen.
        // In diesem Beispiel wissen wir: Wenn sich an einer bestimmten
        // Position ein Leerzeichen befindet, liegt eine Transaktion vor.
        if (ps.getText(new Position(row, 8), 1) !== ' ') {
          transactionCount++;
        }
        // Daten in Spalte 2 prüfen.
        if (ps.getText(new Position(row, 49), 1) !== ' ') {
          transactionCount++;
        }
      }
    }

    // Nach dem Durchlaufen aller Datensatzseiten die Anzahl der Datensätze in einem Meldefenster anzeigen.
    yield ui.message('Es wurden ' + transactionCount + ' für Ihre Konto ' + accountNumber + ' gefunden.');

    // Log out of the application
    ps.sendKeys(ControlKey.PF13);
    ps.sendKeys(ControlKey.PF12);

    // The try / catch allows all errors to be caught and reported in a central location
  } catch (error) {
    // Here we use the ui object to display a message that an error occurred
    yield ui.message(error.message);
  }
});
```

```
// Here we run the macro and return the results to the Macro Runner
// The return statement is required as the application leverages
// this to know if the macro succeeded
return macro();
```

5.9.4 Aufrufen eines Webdienstes

Dieses Beispiel zeigt, wie direkt über ein Makro ein AJAX / REST-Aufruf an einen Webdienst ausgeführt wird. Sie können Daten über Ihre Hostanwendung in den Aufruf des Webdienstes oder umgekehrt über den Webdienst in Ihre Hostanwendung integrieren.

In diesem Beispiel wird der 'Verastream Host Integrator (VHI) CICSAcctsDemo REST'-Dienst aufgerufen. Sie können den Code natürlich auch problemlos anpassen und einen anderen Webdienst aufrufen. Sie sind nicht an den VHI-Dienst gebunden.

In diesem Beispiel wird der Aufruf über einen im Sitzungsserver konfigurierten Proxy durchgeführt (wie unten beschrieben), um „Same-Origin-Policy“-Komplikationen zu vermeiden. Wenn Sie einen Webdienst verwenden, der Cross-Origin Resource Sharing (CORS) unterstützt, und wenn Sie einen modernen Browser verwenden, ist der Proxy nicht erforderlich.

Die jQuery-Bibliothek ist in Makros verfügbar. Sie können zum Aufrufen von REST-Diensten also direkt die $.post()-Funktion verwenden.

In dem Beispiel wird außerdem beschrieben, wie ein jQuery REST-Aufruf in einem neuen Promise-Muster umbrochen wird. Das über die nachstehende benutzerdefinierte Funktion zurückgegebene promise-Muster ermöglicht die Verwendung von „yield“ im Hauptmakrocode. Dadurch kann die Hauptmakroausführung warten, bis der Dienstaufruf abgeschlossen ist, bevor sie fortgesetzt wird.

```
var macro = createMacro(function*() {
 'use strict';

 // Einige Variablen für eine spätere Verwendung erstellen;
 var username;
 var password;
 var accountNumber;
 var accountDetails;

 // Eine Funktion erstellen, die einen AJAX / REST-Aufruf an einen VHI-Webdienst ausführt.
 // Kann für den Aufruf eines beliebigen Webdienstes (nicht nur VHI) angepasst werden.
 // Wenn nicht CORS verwendet wird, muss die Anforderung wahrscheinlich einen
 // Proxy auf dem Sitzungsserver durchlaufen. Siehe Beispielhinweise für weitere Informationen.
 /**
  * Hartcodierte Unterstützungsfunktion zum Einschließen von AJAX / REST-Parametern, zum Aktivieren des
  * REST-Dienstes und zum Zurückgeben der Ergebnisse in einem Promise-Objekt.
  * @param {Number} Kontonummer zum Senden an die REST-Abfrage.
  * @param {String} Benutzername für den Zugriff auf den REST-Dienst.
  * @param {String} Passwort für den Zugriff auf den REST-Service.
  * @return {Promise} enthält $.post()-Ergebnisse, die mit yield kompatibel sind.
 */
 var getAccountDetails = function (acctNum, username, password) {
   var url = "proxy1/model/CICSAcctsDemo/GetAccountDetail";
   var args = {"filters": {"AcctNum": acctNum}, "envVars": {"Username": username, "Password": password}};

   // jQuery AJAX / HTTP POST-Aufruf in einem neuen Promise-Objekt umbrechen.
   // Das hier zurückgegebene Promise-Objekt ermöglicht dem Makro über yield / wait
   // auf seinen Abschluss zu warten.
   return Promise.resolve($.post(url, JSON.stringify(args)))
     .catch(function (error) {
     // Fehler zuordnen, die im jQuery-Aufruf an unser Promise-Objekt auftreten.
     throw new Error('REST API Error: ' + error.statusText);
   });
 };

 // Start generiertes Makro
 var ps = session.getPresentationSpace();
 try {
   // Konnte hier mit dem Host interagieren, sich bei einer Hostanwendung anmelden usw.
   // Benutzername und Passwort erfassen
   username = yield ui.prompt('Username:');
   password = yield ui.prompt('Passwort:', null, true);
   accountNumber = yield ui.prompt('Kontonummer:');
   if (!username || !password || !accountNumber) {
     throw new Error('Kein Benutzername oder Passwort angegeben');
```

```
    }

    // Externen REST-Dienst aktivieren, und yields / wartet auf den Abschluss des Aufrufs.
    accountDetails = yield getAccountDetails(accountNumber, username, password);

    // Jetzt haben wir die Daten von unserem externen Dienst.
    // Können die Daten in unsere lokale Hostanwendung integrieren oder die Daten einfach dem Benutzer anzeigen.
    // In diesem Beispiel zeigen wir einfach die sich ergebenden Kontodetails an.
    if (accountDetails.result && accountDetails.result.length > 0) {
      yield ui.message(accountDetails.result[0].FirstName + ' $' + accountDetails.result[0].AcctBalance);
    } else {
      yield ui.message('Kein Datensatz für folgendes Konto gefunden: ' + accountNumber);
    }
  } catch (error) {
    // Wenn während des AJAX / REST-Aufrufs
    // oder beim Erfassen von Benutzername/Passwort ein Fehler auftritt, befinden wir uns hier.
    yield ui.message(error.message);
  }
  });

// Unser Makro ausführen
return macro();
```

Proxy-Unterstützung für die Skripterstellung aus verschiedenen Ursprüngen

Bei Webdiensten, die CORS nicht unterstützen, treten bei AJAX/REST-Aufrufen Fehler auf, wenn sie versuchen, auf einen nicht aus der Host Access for the Cloud-Anwendung stammenden Server zuzugreifen. Dabei handelt es sich um eine Browser-Sicherheitsfunktion.

Der Host Access for the Cloud-Server bietet eine Möglichkeit, explizit einen Proxy zu verbürgten Remoteservern bereitzustellen.

- Öffnen Sie `..\<Installationsverzeichnis>\sessionserver\microservice\sessionserver\service.yml` zur Bearbeitung.
- Fügen Sie im Abschnitt `env` Folgendes hinzu:

  ```
  name: zfe.proxy.mappings
  value: proxy-path=proxy-to-address
  ```

  Dabei bezieht sich `proxy-path` auf die gewünschte URL-Zuordnung und `proxy-to-address` auf die URL, bei der der Aufruf über einen Proxy gesendet wird.
- In diesem Beispiel:

  ```
  name: zfe.proxy.mappings
  value: proxy1=http://remote-vhi-server:9680/vhi-rs/
  ```

  Aufrufe für `<Server:Port>/proxy1` werden über einen Proxy an `http://remote-vhi-server:9680/vhi-rs/` gesendet.
- Mehrere Proxyzuordnungen können angegeben werden, indem die einzelnen Zuordnungen durch ein Komma getrennt werden.
- Bitte beachten Sie: Ein REST-Server unterstützt zwar CORS-Titel, ältere Browser tun dies jedoch nicht. Daher kann dieses Beispiel weiterhin relevant sein.

> **Tipp**
>
> Die Datei `service.yml` kann ersetzt werden, wenn Sie Host Access for the Cloud neu bereitstellen. Denken Sie daran, immer Ihre Dateien zu sichern.

5.9.5 Arbeiten mit Datenzellen und Attributen

Dieses Makro veranschaulicht, wie Sie Datenzellen und Attributsätze zum Überprüfen einer bestimmten Zeile/Spalte auf dem Bildschirm für Text und Attribute verwenden können. In diesem Beispiel sehen Sie Folgendes:

- Wie Sie eine Sammlung von DataCells-Objekten für eine bestimmte Position und Länge abrufen.
- Wie Sie DataCells-Objekte zum Erstellen einer Textzeichenfolge durchlaufen.
- Wie Sie zum Vergleich in ähnlicher Weise auch getText() verwenden können.
- Wie Sie mit Attributen arbeiten, eine Auflistung mit Zeichenfolgen abrufen oder feststellen, ob bestimmte Attribute an einer festgelegten Bildschirmposition angegeben sind.

```
var macro = createMacro(function*() {
    'use strict';

    // Präsentationsbereich für die Interaktion mit dem Host abrufen
    var ps = session.getPresentationSpace();

    // Variablen für eine spätere Verwendung deklarieren
    var cells;
    var text;
    var attrs;

    // Standardwartezeit für "wait"-Funktionen festlegen
    wait.setDefaultTimeout(10000);

    // Beispielmakro für das Arbeiten mit Datenzellen und Attributen
    try {
        yield wait.forCursor(new Position(24, 2));

        // Datenzellen aus dem Präsentationsbereich abrufen
        // Zeile 19, Spalte 3 ist die Eingabeaufforderung 35 Zeichen lang
        // "Wählen Sie einen der folgenden Befehle:"
        cells = ps.getDataCells({row:19, col:3}, 35);
        text = '';

        // Sie können Text mithilfe von 'getText' anzeigen
        yield ui.message("Screen text: " + ps.getText({row:19, col:3}, 35));

        // Oder den Text aus den Datenzellen an den einzelnen Positionen bilden
        for(var index = 0; index < cells.length; index++) {
            text = text.concat(cells[index].getChar());
        }
        // Und den Text anzeigen
        yield ui.message("Cells text: " + text);

        // Attribute für die erste Datenzelle abrufen (cell[0])
        attrs = cells[0].getAttributes();

        // Anzeigen, ob Attribute für die Datenzelle vorhanden sind
        yield ui.message("Attribute set is empty: " + attrs.isEmpty());

        // Anzeigen, wie viele Attribute angegeben sind
        yield ui.message("Number of attributes: " + attrs.size());

        // Anzeigen, welche Attribute angegeben sind
        yield ui.message("Attributes: " + attrs.toString());

        // Anzeigen, ob das das Attribut 'HIGH_INTENSITY' angegeben ist
        yield ui.message("Is high intensity: " +
                         attrs.contains(Attribute.HIGH_INTENSITY));

        // Anzeigen, ob das Attribut 'UNDERLINE' angegeben ist
        yield ui.message("Is underline: " +
                         attrs.contains(Attribute.UNDERLINE));

        // Anzeigen, ob die Attribute 'ALPHA_NUMERIC', 'HIGH_INTENSITY' und 'PEN_DETECTABLE' angegeben sind
```

```
        yield ui.message("Is alphanumeric, intensified and pen-detectable: " +
                         attrs.containsAll([Attribute.ALPHA_NUMERIC, Attribute.HIGH_INTENSITY, Attribute.PEN_DETECTABLE]));

        // Anzeigen, ob die Attribute 'UNDERLINE', 'HIGH_INTENSITY' und 'PEN_DETECTABLE' angegeben sind
        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);
    }
 //Generiertes Makro beenden
});

// Zurückgegebenes Makro ausführen
return macro();
```

5.9.6 Verwenden von Feldern und Feldlisten

Dieses Makrobeispiel veranschaulicht die Verwendung allgemeiner Funktionen für die Interaktion mit den Feldern in der Makro-API. Es wird beispielsweise dargestellt, wie Feldtext abgerufen wird, Feldinformationen angezeigt werden und wie field.setText als Alternative zu sendKeys für die Interaktion mit dem Host verwendet werden kann.

> **Hinweis**
>
> Aufgrund bestimmter Browseraspekte reduziert `ui.message` mehrere aufeinander folgende Leerzeichen zu einem einzelnen Leerzeichen. Die Leerzeichen werden im JavaScript-Code beibehalten.

```
var macro = createMacro(function*() {
    'use strict';

    // Präsentationsbereich für die Interaktion mit dem Host abrufen
    var ps = session.getPresentationSpace();

    // Variablen für eine spätere Verwendung deklarieren
    var fields;
    var field;
    var searchString = 'z/VM';

    // Standardwartezeit für "wait"-Funktionen festlegen
    wait.setDefaultTimeout(10000);

    // Beispielmakro für das Arbeiten mit Feldlisten und Feldern
    try {
        yield wait.forCursor(new Position(24, 2));

        // Feldliste abrufen.
        fields = ps.getFields();

        // Die gesamte Feldliste durchlaufen und Feldinfo anzeigen.
        for(var index = 0; index < fields.size(); index++) {
            field = fields.get(index);

            yield ui.message("Field " + index + " info: " + field.toString());
        }

        yield ui.message("Hier ein Feld mit dem 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()));
        }

        // Jetzt nach einem Befehlsfeld suchen und es ändern.
        field = fields.findField(new Position(23, 80));
        if(field !== null) {
            field.setText("cics");
        }

        yield ui.message("Klicken Sie mit der Maus, um 'cics' an den Host zu senden.");
        ps.sendKeys(ControlKey.ENTER);

        // Auf neuen Bildschirm warten; neue Felder abrufen.
        yield wait.forCursor(new Position(10, 26));
        fields = ps.getFields();

        // Benutzerfeld suchen und festlegen.
        field = fields.findField(new Position(10, 24));
        if(field !== null) {
```

```
            field.setText("myusername");
        }
        // Passwortfeld suchen und festlegen.
        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);

        // Auf neuen Bildschirm warten; neue Felder abrufen.
        yield wait.forCursor(new Position(1, 1));
        fields = ps.getFields();

        // Befehlsfeld suchen und 'logoff'-Befehl festlegen.
        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);
    }
    //Ende generiertes Makro

});

// Makro ausführen
return macro();
```

5.9.7 Makro für die automatische Anmeldung für Mainframes

In diesem Beispiel wird mit dem AutoSignon-Objekt ein Makro erstellt, das die einem Benutzer zugeordneten Berechtigungsnachweise verwendet, um ein Weiterleitungsticket vom Digital Certificate Access Server (DCAS) abzurufen.

```
var macro = createMacro(function*() {
    'use strict';

    // Präsentationsbereich für die Interaktion mit dem Host abrufen
    var ps = session.getPresentationSpace();

    // Variable für Weiterleitungsticket für die Anmeldung
    var passTicket;

    // Anwendungs-ID für die Anmeldung
    var appId = 'CICSV41A';

    // Standardwartezeit für "wait"-Funktionen festlegen
    wait.setDefaultTimeout(10000);

    // Start generiertes Makro
    try {
    yield wait.forCursor(new Position(24, 2));

       // Weiterleitungsticket von DCAS abrufen.
       passTicket = yield autoSignon.getPassTicket(appId);

        ps.sendKeys('cics');
        ps.sendKeys(ControlKey.ENTER);

        yield wait.forCursor(new Position(10, 26));

        // Generierten Benutzernamen mit 'sendUserName(passTicket) ...' ersetzen
        yield autoSignon.sendUserName(passTicket);

        // ps.sendKeys('bvtst01' + ControlKey.TAB + ControlKey.TAB);
        ps.sendKeys(ControlKey.TAB + ControlKey.TAB);

        yield wait.forCursor(new Position(11, 26));

        // Generiertes Passwort mit 'sendPassword(passTicket) ...' ersetzen
        yield autoSignon.sendPassword(passTicket);

        // var userInput3 = yield ui.prompt('Passwort:', '', true);
         // if (userInput3 === null) {
             // throw new Error('Kein Passwort angegeben');
        // }
        // ps.sendKeys(userInput3);
        ps.sendKeys(ControlKey.ENTER);

        yield wait.forCursor(new Position(1, 1));
        yield ui.message('Angemeldet. Melde mich ab.');
        ps.sendKeys('cesf logoff');
        ps.sendKeys(ControlKey.ENTER);
    } catch (error) {
        yield ui.message(error);
```

```
    }
    //Ende generiertes Makro
});

// Makro ausführen
return macro();
```

5.9.8 Verwenden der Dateiübertragung (IND$File)

Mit den folgenden Beispielmakros wird veranschaulicht, wie Sie mithilfe der Dateiübertragungs-API eine Dateiliste abrufen, eine Datei herunterladen und eine Datei auf einen 3270-Host hochladen können.

> **Hinweis**
>
> Zum Ausführen dieser Makros müssen Sie angemeldet sein und eine Eingabeaufforderung geöffnet haben.

- Makro zum Auflisten von Dateien
- Makro zum Herunterladen einer Datei
- Makro zum Hochladen einer Datei

Makro zum Auflisten von Dateien

Mit diesem Makro wird veranschaulicht, wie Sie mithilfe der Dateiübertragungs-API mittels IND$File-Übertragung eine Dateiliste auf einem 3270-Host abrufen. Das IND$File-Übertragungsobjekt wird aus der Dateiübertragungsfactory abgerufen und dann zum Abrufen eines Arrays von HostFile-Objekten von TSO oder CMS verwendet.

```
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 = 'Der Katalogname lautet ' + firstFile.getParent() + '. ';
            var msg2 = 'The first file is ' + firstFile.getName();
            yield ui.message(msg1 + msg2);
        }
    } catch (error) {
        yield ui.message(error);
    }
});

// Makro ausführen
return macro();
```

Makro zum Herunterladen einer Datei

Mit diesem Makro wird veranschaulicht, wie Sie mithilfe der Dateiübertragungs-API mittels IND$File-Übertragung eine Datei von einem 3270-Host herunterladen. Das IND$File-Übertragungsobjekt wird aus der Dateiübertragungsfactory abgerufen. In diesem Beispiel ist ASCII als Übertragungsmethode festgelegt, um die Verwendung der setTransferOptions-Funktion zu veranschaulichen.

Das Beispielmakro lädt die erste Datei herunter, die von einem Aufruf an getHostFileListing zurückgegeben wurde, indem ein Download-URI mit einem Aufruf der getDownloadUrl-Funktion erstellt wird. Das Makro kann entweder in einer CMS- oder TSO-Umgebung verwendet werden, aber die Auswahl muss in der ersten Zeile angegeben oder der Code für das beabsichtigte System leicht geändert werden.

```
var hostEnvironment = 'CMS';  // 'TSO'
// Dateipfad erstellen, d. h. catalog/file.name oder 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();

        // transferMethod-Optionen sind 'binary' und 'ascii'
        fileTransfer.setTransferOptions({transferMethod: 'ascii'});

        // In dieser Demo wird die erste Datei abgerufen, die in der Liste
        var hostFiles = yield fileTransfer.getHostFileListing();
        var firstHostFile = hostFiles[0];

        if (hostEnvironment === 'CMS') {
           yield wait.forText('Ready', new Position(1,1), 5000);
        }

        // Download
        // Wenn Ihnen der Pfad der gewünschten Datei bereits bekannt ist, übergeben Sie ihn einfach an getDownloadURL()
        var downloadUrl = fileTransfer.getDownloadURL(getPath(firstHostFile));

        // Dadurch wird der Browserspeicherort geändert. Möglicherweise ergeben sich unterschiedliche Ergebnisse in unterschiedlichen
Browsern.
        window.location = downloadUrl;

        // Wenn Sie die Dateiinhalte in eine Variable einlesen möchten, anstatt sie
        // herunterzuladen, können Sie Folgendes verwenden: jQuery
        // var fileContents = yield $.get(downloadUrl);

    } catch (error) {
         yield ui.message(error);
    }
    });

// Makro ausführen
return macro();
```

Makro zum Hochladen einer Datei

Mit diesem Makro wird veranschaulicht, wie Sie mithilfe der Dateiübertragungs-API mittels IND$File-Übertragung eine Datei auf einen 3270-Host hochladen. Mit dem Beispielmakro wird der Benutzer aufgefordert, eine Datei im lokalen Dateisystem auszuwählen, indem das Dialogfeld des Browsers zur Dateiauswahl ausgelöst wird. Dann wird durch Aufrufen von getHostFileListing der aktuelle Katalog auf TSO oder die Laufwerkskennung auf CMS abgerufen. Schließlich wird die sendFile-Funktion aufgerufen, um die ausgewählte lokale Datei an den Host zu übermitteln.

Das Makro kann entweder in einer CMS- oder TSO-Umgebung verwendet werden, aber die Auswahl sollte in der ersten Zeile angegeben werden. In diesem Beispiel ist die Übertragungsart auf **ascii** festgelegt. Sie können dies jedoch in **binary** ändern.

```
var hostEnvironment = 'CMS';  // 'TSO'
 // Dialogfeld des Browsers zur Dateiauswahl programmgesteuert öffnen
function promptForFileToUpload () {
    return new Promise(function (resolve, reject) {
        // Es erfolgt keine Benachrichtigung, wenn der Benutzer das Dialogfeld zur Dateiauswahl schließt, daher nach 30 Sekunden ablehnen
        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();

       // transferMethod-Optionen sind 'binary' und 'ascii'
        fileTransfer.setTransferOptions({transferMethod: 'ascii'});

        var localFile = yield promptForFileToUpload();

        // Aktuellen Katalognamen abrufen und ausgewählten Dateinamen an ihn anfügen
        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);
    }
});

 // Makro ausführen
return macro();
```

5.10 Ausführen von Makros bei Ereignissen

Im Bereich „Makro“ können Sie die auszuführenden Makros und den Zeitpunkt der Ausführung auswählen.

- Makro beim Start ausführen – Wählen Sie ein Makro, das beim Sitzungsstart automatisch ausgeführt wird.
- Makro beim Verbinden ausführen – Wählen Sie ein Makro, das automatisch ausgeführt wird, wenn die Sitzung eine Verbindung zum Host herstellt.
- Makro beim Trennen der Verbindung ausführen – Wählen Sie ein Makro, das automatisch ausgeführt wird, wenn die Verbindung der Sitzung zum Host getrennt wird.

Weitere Informationen

- Erstellen von Makros
- Verwenden der Makro-API
- Beispielmakros

5.11 Druckvorgang

Verschiedene Druckoptionen für 3270-, 5250- und UTS-Hosts stehen zur Verfügung. Sie können Bildschirmaufnahmen erstellen, einen ausgewählten Bildschirm drucken und Host-Druckfunktionen aktivieren und konfigurieren:

Die verfügbaren Einstellungen für die Einrichtung der Seite und der Ausrichtung hängen von den Browsereinstellungen ab.

5.11.1 Erfassen von Bildschirmen

Verwenden Sie die Funktion für Bildschirmaufnahmen, um mehrere Bildschirme zu erfassen und dann als Datei zum Drucken oder zur Freigabe zu speichern. Diese Option ist für alle Benutzer verfügbar, wenn der Administrator sie in den **Benutzereinstellungen** auswählt.

1. Navigieren Sie zu dem Bildschirm, den Sie erfassen möchten.
2. Klicken Sie auf  , um den Bildschirm zu erfassen. Im Zähler wird die Anzahl der erstellten Bildschirmaufnahmen angezeigt. Jede Aufnahme wird in einer separaten Seite gedruckt.
3. Klicken Sie auf „Speichern“, um zu dem Speicherort zu navigieren, in dem die Aufnahme gespeichert werden soll. Die Optionen zum Speichern hängen vom jeweils verwendeten Browser ab. In Chrome wird die Datei abhängig von den Browsereinstellungen beispielsweise im Downloadordner gespeichert, oder es wird das Dialogfeld „Speichern unter“ angezeigt, in dem ein Speicherort für die Datei ausgewählt werden kann.
4. Um die neu gespeicherten Bildschirmaufnahmen in einer vorhandenen Datei für Bildschirmaufnahmen anzufügen, klicken Sie auf **Anfügen und speichern**. Wenn Sie die angefügte Datei drucken, wird jede Bildschirmaufnahme in einer separaten Seite gedruckt.
5. Sie können die Bildschirmaufnahmen jederzeit durch Klicken auf **Löschen** löschen.

5.11.2 Drucken von Bildschirminhalten

Die Inhalte des Terminalbildschirms werden über die Option „Bildschirminhalt drucken“ gedruckt. Die Symbolleiste oder sonstige Anzeigeinformationen sind in dem Druckauftrag nicht enthalten.

1. Navigieren Sie zu dem Bildschirm, den Sie drucken möchten.
2. Klicken Sie in der Symbolleiste auf „Bildschirminhalt drucken“.
3. Verwenden Sie im Browser das Dialogfeld für Druckvorgänge, um die Einstellungen für den Drucker und die Einrichtung der Seite auszuwählen.

5.11.3 Hostdruck

Diese Funktion ist in 3270-, 5250- und UTS-Hostsitzungen verfügbar. Sie können eine oder mehrere -Druckersitzungen erstellen und der aktuellen -Terminalsitzung zuordnen. Jede Druckersitzung ist an eine Geräte-ID auf dem Hostsystem gebunden und alle nachfolgenden an diese Geräte-ID gesendeten Druckaufträge werden an den Host Access for the Cloud-Webclient geleitet.

Die Hostsitzung erstellt eine PDF-Datei mit dem Inhalt der zu druckenden Datei und sendet diese an den Webclient. Nach dem Empfang der Datei wird diese auf dem Webclient entsprechend den konfigurierten Downloadoptionen des Browsers heruntergeladen. Unterschiedliche Browser umfassen unterschiedliche Optionen zum Verarbeiten heruntergeladener Dateien. Nach dem Empfang der PDF-Datei können Sie sie an jeden Drucker weiterleiten, auf den Sie Zugriff haben.

> **Hinweis**
>
> Über die Option **Hostdruck** in den Benutzereinstellungen kann ein Administrator für Endbenutzer die Möglichkeit zum Drucken festlegen.

So konfigurieren Sie den -Hostdruck

1. Klicken Sie in einer Hostsitzung in der Symbolleiste auf **Einstellungen**, um den linken Navigationsbereich zu öffnen.
2. Klicken Sie im linken Bereich auf **Drucken**.
3. Klicken Sie auf **Hinzufügen**, um das Dialogfeld „Konfiguration“ zu öffnen. Passen Sie Ihre Druckersitzung an, indem Sie die Einstellungen auf jeder Registerkarte verwenden: Verbindungseinstellungen, Einstellungen für „Seite einrichten“, erweiterte Einstellungen.
4. Klicken Sie auf **Speichern**, um zur Sitzung zurückzukehren. Die Einstellungen werden wirksam, nachdem die Sitzung erneut geöffnet wurde.

Themen zum Hostdruck

- Verbindungseinstellungen: 3270, 5250, UTS
- Einstellungen für „Seite einrichten“
- Erweiterte Einstellungen
- So drucken Sie Ihre Host-Druckersitzung

Verbindungseinstellungen

Standardmäßig sind Druckersitzungen über das Druckersymbol in der Symbolleiste der Terminalsitzung verfügbar. Wenn Endbenutzer keinen Zugriff auf eine bestimmte Druckersitzung haben sollen, deaktivieren Sie die Option **Diese Druckersitzung aktivieren** auf der Registerkarte „Verbindung“.

Diese Einstellungen variieren je nach Hosttyp.

- 3270-Verbindungseinstellungen
- 5250-Verbindungseinstellungen
- UTS-Verbindungseinstellungen

3270-VERBINDUNGSEINSTELLUNGEN

Einstellung	Beschreibung
Name	Geben Sie einen leicht erkennbaren Namen für die Druckersitzung ein. Erforderlich.
Protokoll	Geben Sie das zu verwendende Protokoll an. Die Optionen sind: • **TN3270E** – TN3270E (eine Telnet Extended-Option) ist für Benutzer von TCP/IP-Software gedacht, die über ein Telnet-Gateway (mit RFC 1647-Implementierung) eine Verbindung zum IBM-Mainframe herstellen. • **TN3287** – TN3287 ist für Benutzer von TCP/IP-Software gedacht, die über ein Telnet-Gateway (mit RFC 1646-Implementierung) eine Verbindung zum IBM-Mainframe herstellen.
Geräte-ID	Geben Sie an, ob Sie eine Geräte-ID, eine Aufforderung für den Gerätenamen oder, bei Auswahl von TN3270E, eine TN-Assoziierung verwenden möchten, um die Terminalsitzung mit der Drucksitzung zu verknüpfen. Erforderlich. Bitte auswählen: • Geräte-ID angeben: Geben Sie die Geräte-ID an, die bei der Verbindung der Druckersitzung zum Host verwendet werden soll. • TN-Assoziierung verwenden: (TN3270E) Wenn Sie sich für eine TN-Assoziierung entscheiden, verwendet Host Access for the Cloud den Gerätenamen, der in den Verbindungseinstellungen angegeben ist, um die 3270- und der 3287-Sitzungen zu verknüpfen. Die TN-Assoziierung ist nur verfügbar, wenn TN3270E als Protokoll ausgewählt wird. • Eingabeaufforderung: Beim Verbinden der Druckersitzung wird der Benutzer aufgefordert, die Geräte-ID für die Druckersitzung anzugeben.

5250-VERBINDUNGSEINSTELLUNGEN

Einstellung	Beschreibung
Name	Geben Sie einen leicht erkennbaren Namen für die Druckersitzung ein. Erforderlich.
Geräte-ID	Geben Sie an, ob Sie eine Geräte-ID verwenden oder eine Eingabeaufforderung für die Geräte-ID anzeigen lassen möchten: • Geräte-ID angeben: Geben Sie die Geräte-ID an, die bei der Verbindung der Druckersitzung zum Host verwendet werden soll. • Eingabeaufforderung: Beim Verbinden der Druckersitzung wird der Benutzer aufgefordert, die Geräte-ID für die Druckersitzung anzugeben.

UTS-VERBINDUNGSEINSTELLUNGEN

Einstellung	Beschreibung
Name	Geben Sie einen leicht erkennbaren Namen für die Druckersitzung ein. Erforderlich.
Protokoll	Die Wahl des DEMAND- oder MAPPER-Protokolls hängt vom Typ der erstellten UTS-Sitzung ab. UTS-Sitzungstypen werden über die Werte bestimmt, die Sie im Verbindungsbereich für die TSAP- und Anwendungsoptionen angeben. Wenn Sie beispielsweise Werte zum Erstellen einer UTS MAPPER- oder DEMAND-Sitzung eingeben, sollten Sie MAPPER oder DEMAND als Protokoll auswählen. Geben Sie an, welches Protokoll verwendet werden soll: • **MAPPER**: Sie können wählen, ob Sie die Geräte-ID für die Verbindung der Druckersitzung mit dem Host angeben möchten oder ob eine Eingabeaufforderung angezeigt werden soll, sodass der Benutzer die Geräte-ID für die Druckersitzung angibt. Fahren Sie dann mit der Konfiguration der Sitzung fort. • **DEMAND**: Nachdem Sie einen Namen für die Sitzung angegeben haben, können Sie mit der Konfiguration der Sitzung auf den Registerkarten „Seite einrichten“ und „Erweitert“ fortfahren.

Einstellungen für „Seite einrichten“

Die Registerkarte „Seite einrichten“ enthält Einstellungsoptionen für Papierformat und Ausrichtung sowie für Abmessungen, Ränder und Skalierungswerte.

Einstellung	Beschreibung
Papierformat	Wählen Sie das im Drucker verwendete Papierformat aus.
Ausrichtung	Wählen Sie aus drei Modi: **Hochformat** (vertikal), **Querformat** (horizontal) oder **Automatisch**. Letzteres ist die Standardeinstellung. Wenn „Automatisch“ ausgewählt ist, wird der Druckauftrag im Drucker ausgewertet und das am besten geeignete Format verwendet.
Maßeinheiten	Wählen Sie die Maßeinheit aus, die Sie für die Seitenränder und die Seitengröße verwenden möchten. Mögliche Werte sind „Zoll“ und „Millimeter“.
Abmessungen	Geben Sie die Anzahl der Zeilen und Spalten ein, die pro Druckseite angezeigt werden. 60 ist der Standardwert für Zeilen und 80 der Standardwert für Spalten.
Ränder	Legt den linken, rechten, oberen und unteren Seitenrand fest.
Skalierung	Legt die horizontale und vertikale Skalierung für die Druckausgabe fest. Erhöhen Sie den Prozentsatz, um den horizontalen oder vertikalen Abstand im Ausdruck zu erhöhen.

Erweiterte Einstellungen

Wählen Sie aus, wann die PDF-Datei heruntergeladen werden soll.

- **Automatisch** (Standardeinstellung) – Die PDF-Datei wird automatisch heruntergeladen, wenn der Druckauftrag abgeschlossen ist. Wenn diese Option ausgewählt ist, ist die Einstellung „Wartezeit bei Inaktivität“ nicht verfügbar.
- **Manuell** – Nachdem ein Druckauftrag gestartet wurde, können Sie jederzeit einen Download initiieren, indem Sie den Druckauftrag in der Downloadliste suchen, die über das Druckersymbol in der Symbolleiste verfügbar ist, und auf „Leeren“ klicken. Der Druckauftrag wird in einer PDF-Datei zusammengeführt und heruntergeladen.
- **Nach Wartezeit bei Inaktivität** – Über diese Option können Sie mehrere Druckaufträge drucken, wobei sie in einer einzelnen PDF-Datei zusammengeführt und dann automatisch zum angegebenen Zeitpunkt heruntergeladen werden können.

  Wenn Sie einen höheren Wert als 0 angeben (z. B. 5 Sekunden), werden alle einem Drucker zugewiesenen Druckaufträge, die innerhalb von 5 Sekunden nacheinander eingehen, an dieselbe PDF-Datei angefügt. Nach 5 Sekunden und wenn keine Druckaufträge mehr vorhanden sind, wird die PDF-Datei heruntergeladen.

  Wenn Sie „0“ für die Wartezeit bei Inaktivität angeben, wird jeder Druckauftrag sofort nach Abschluss heruntergeladen. Sie haben immer die Möglichkeit, einen Druckauftrag zu unterbrechen, indem Sie auf **Leeren** klicken.

So drucken Sie Ihre Host-Druckersitzung

Nach dem Öffnen der Terminalsitzung haben Sie folgende Möglichkeiten:

1. Wählen Sie die zu verwendende Druckersitzung aus. Ihnen stehen alle Druckersitzungen zur Verfügung, die der geöffneten Terminalsitzung zugeordnet sind. Klicken Sie in der Symbolleiste auf  , um eine Liste anzuzeigen.
2. Die Hostsitzung empfängt die Druckdaten vom Host und erstellt eine PDF-Datei für den Druck. Eine Verknüpfung zu dieser Datei wird an den Webclient gesendet und gibt an, dass sie zum Herunterladen verfügbar ist.

   Sie können die verschiedenen Druckaufträge über den Seitenzähler der Symbolleiste oder den Zähler überwachen, der den einzelnen Druckern in der Dropdownliste zum Drucken zugeordnet ist.

   Der Seitenzähler in der Symbolleiste gibt die Gesamtzahl der Seiten an, die entweder aktiv gedruckt werden oder abgeschlossen sind, für die das Herunterladen der entsprechenden Datei vom Server jedoch noch aussteht. Durch Auswählen von „Leeren“ in der Druckerliste können Sie einen Download auslösen.

   Der den Druckern in der Dropdownliste der Drucker zugeordnete Seitenzähler zeigt denselben, jedoch nach einzelnen Druckern aufgeschlüsselten Wert an. Die Summe dieser einzelnen Druckaufträge wird im Zähler in der Symbolleiste angegeben. Der Zähler wird gelöscht, nachdem die Druckaufträge heruntergeladen wurden.
3. Nachdem die PDF-Datei zur Verfügung steht, wird sie entweder heruntergeladen, oder es wird gewartet, dass Sie über die Option „Leeren“ einen Download auslösen. Dies hängt von den Optionen ab, die Sie konfiguriert haben.

Bei Bedarf können Sie aufgrund eines allzu lang ausgeführten Druckauftrags oder eines anderen Problems den aktuellen Druckauftrag leeren. Die Option **Leeren** ist in der Liste der Druckersitzungen verfügbar, die über das Druckersymbol in der Symbolleiste angezeigt wird. Wenn Sie einen Druckauftrag leeren, werden zunächst noch alle bis dahin aufgelaufenen Daten fertig gedruckt. Anschließend wird die Verarbeitung von Druckdaten fortgesetzt.

6. Entwicklung

6.1 Entwicklung

Host Access for the Cloud umfasst eine Sammlung von APIs und Bibliotheken, mit denen Sie leistungsfähige Client/Server- und Webanwendungen entwickeln können, mit denen Hostdaten in verschiedene Entwicklungsumgebungen integriert werden.

Sie können außerdem den Webclient erweitern, ohne die installierten Dateien zu beeinträchtigen. Diese Funktion bietet Ihnen zahlreiche Optionen zum Anpassen des Webclients an Ihre Anforderungen.

- Durch Verwenden des Java-SDK können Sie die bereitgestellte Java-API verwenden, um die Darstellung von Hostdaten mithilfe serverseitiger Ereignisse zu verbessern.
- Durch Verwenden von Connector for Windows können Sie mithilfe der API und der bereitgestellten Beispiele mit Hostsitzungen in Ihrer .NET-Anwendung oder innerhalb von Visual Basic for Applications interagieren.
- Durch Verwenden der JavaScript-API können Sie den Webclient in Ihre eigene Website einbetten.
- Durch Erweitern des Webclients können Sie den Umfang des Webclients mit benutzerdefiniertem Code wie CSS oder JavaScript erweitern.

HACloud-API-Dokumentation

6.2 Verwenden des Java-SDK

Durch Verwendung von serverseitigen Ereignissen und des Host Access for the Cloud-SDK können Sie prozeduralen Java-Code bereitstellen, mit dem die Darstellung von Hostdaten erweitert und verbessert wird. Zur Unterstützung bei der Erstellung serverseitiger Ereignisse verfügt Host Access for the Cloud über ein SDK und Beispiele, die Sie als Ausgangspunkt nutzen können.

Die Javadoc-Dateien sind im Installationsverzeichnis (`<Installationsverzeichnis>\sessionserver\sdk\java\javadocs\index.html`) und online unter HACloud Javadocs verfügbar.

1. Machen Sie das Host Access for the Cloud-SDK für Ihre Entwicklungsumgebung verfügbar. Das SDK ist unter \sessionserver\sdk verfügbar.
2. Schreiben Sie den für die Aufgabe erforderlichen Java-Code und kompilieren Sie den Code in einer JAR-Datei (Java Archive) in eine Java-Klasse.
3. Kopieren Sie die JAR-Datei in das Verzeichnis `<Installationsverzeichnis>\sessionserver\microservices\sessionserver\extensions\server` und starten Sie den Sitzungsserver neu.

   Wenn das Ereignis auf mehreren Servern ausgeführt werden soll, kopieren Sie die JAR-Datei auf den jeweiligen Servern in das entsprechende Verzeichnis.
4. Fügen Sie die Sitzung hinzu, die Sie dem Ereignis in der Verwaltungskonsole zuordnen möchten.
5. Öffnen Sie beim Konfigurieren der Sitzung im Webclient den Bereich „Anpassung“ und geben Sie den vollständigen Klassennamen für das Ereignis ein.
6. Starten Sie die Sitzung und testen Sie das Ereignis.

6.2.1 Beispiele und Dokumentation

So greifen Sie auf das SDK zur direkten Anzeige zu und importieren es in die IDE:

1. Navigieren Sie zu `<Installationsverzeichnis>\sessionserver\sdk\java`
2. Greifen Sie im SDK-Verzeichnis auf die folgenden Unterverzeichnisse zu:

   - `\javadoc` – Dieses Verzeichnis enthält Javadoc-Dateien zur direkten Ansicht.
   - `\samples` – Dieses Verzeichnis enthält Java-Quelldaten zur direkten Ansicht.
   - `\zfe-sdk.jar` – Die JAR-Datei enthält Java-Klassen zum Import in Ihre Java-Entwicklungsumgebung (IDE).
   - `\zfe-sdk-javadoc.jar` – Die JAR-Datei enthält JavaDoc-Dateien zum Import in Ihre IDE.

6.3 Verwenden von Connector for Windows

Host Access for the Cloud Connector for Windows ist eine separate Installation, die auf der Download-Website von Micro Focus verfügbar ist. Mit Connector for Windows können Sie in einer .NET-Anwendung oder in Visual Basic for Applications mit Hostsitzungen interagieren.

Die API-Dokumentation ist in Ihrem Installationsverzeichnis (`<Installationsverzeichnis>\sessionserver\sdk\csharp\apidocs\index.html`) und online unter HACloud Connector for Windows verfügbar.

Einige Punkte sind bei der Vorbereitung zur Installation zu berücksichtigen:

- Es sind zwei Installationsplattformen verfügbar: eine 32-Bit-Version und eine 64-Bit-Version. Je nachdem, welche Version Sie installieren, lautet der Standardpfad für die Basisinstallation `C:\Programme (x86)\Micro Focus\HACloud\Connector for Windows` oder `C:\Programme\Micro Focus\HACloud\Connector for Windows`
- Durch die ausgewählte Installationsplattform wird auch die Lösungsplattform für die Entwicklung vorgegeben. Beispiel: Wenn Sie die 32-Bit-Version von Microsoft Office® installiert haben und Visual Basic for Applications mit dem Connector verwenden möchten, müssen Sie die 32-Bit-Version von Host Access for the Cloud Connector for Windows installieren.
- Die API-Dokumentation ist verfügbar in: `<Installationsverzeichnis>\sessionserver\sdk\csharp\apidocs\index.html`
- .NET 4.5.2 ist erforderlich.
- Der Connector für Windows unterstützt zwei Authentifizierungsmethoden: LDAP und „Keine“. Die Authentifizierung wird in der MSS-Verwaltungskonsole konfiguriert.

6.3.1 Beispiele und Dokumentation zum Connector

Die Dokumentation ist zur Referenz für Ihre IDE verfügbar. Zudem stehen Beispiele zur Verwendung des Connectors zur Verfügung. Die Dokumentation und die Beispiele finden Sie hier:

1. Navigieren Sie zum Installationsverzeichnis. In einer Standardinstallation abhängig von der verwendeten Plattform entweder `C:\Programme (x86)\Micro Focus\HACloud\Connector for Windows` oder `C:\Programme\Micro Focus\HACloud\Connector for Windows`.
2. Im Connector for Windows-Verzeichnis finden Sie Folgendes:
    - `MicroFocus.ZFE.Connector.dll` – Eine .NET Framework-Assembly zum Verweis in Ihrem C#- oder .NET-Projekt.
    - `MicroFocus.ZFE.Connector.tlb` – Eine Typbibliothek zur Verwendung in Ihrem COM- oder Visual Basic for Applications-Projekt.
    - `\help` – Dieses Verzeichnis enthält Hilfeinformationen zur Verwendung des Connectors.
    - `\samples` – Dieses Verzeichnis enthält die Codebeispiele, die als Ausgangspunkt zum Entwickeln Ihrer eigenen Anwendungen dienen.

6.3.2 Verwenden des Connectors mit Microsoft Visual Studio

Wenn Sie Microsoft Visual Studio für die Entwicklung von Anwendungen verwenden, sollten Sie Folgendes berücksichtigen:

- Stellen Sie bei Verwendung von Microsoft Visual Studio mit Connector for Windows sicher, dass die Lösungsplattform je nach Installation entweder auf x86 oder x64 festgelegt ist. Aufgrund der im Connector for Windows-SDK verwendeten nativen Komponenten wird die Plattform „Any CPU“ (Beliebige CPU) nicht unterstützt. Verwenden Sie den Konfigurations-Manager für die Visual Studio-Lösung zum Erstellen einer Plattform für x86 oder x64.
- Beim Hinzufügen eines Verweises auf die Connector for Windows-Bibliothek wird in Visual Studio die Eigenschaft „Copy Local“ (Lokal kopieren) möglicherweise auf „True“ (Wahr) festgelegt. Die Eigenschaft muss auf „False“ (Falsch) festgelegt werden, sodass die Bibliothek und ihre Abhängigkeiten über das Installationsverzeichnis des SDK ausgeführt werden.

6.4 Verwenden der JavaScript-API

Durch Verwenden von JavaScript in einem Browser können Sie den Webclient in eine Webseite einbetten. Die Endbenutzer können dann über eine herkömmliche Webseite mit dem Webclient interagieren und eine Verbindung zur Hostanwendung herstellen, die Folgendes ermöglicht:

- Programmatische Interaktion mit Hostsitzungen
- „Monitorloses“ Ausführen, d. h. Ausführen mit Zugriff auf die gesamte Funktionalität ohne sichtbare Benutzeroberfläche, die in die Webseite eingebettet ist

Tutorials zu den ersten Schritten und weitere Tutorials stehen zur Verfügung. Die API-Dokumentation und die Tutorials sind online unter HACloud JavaScript API und in `<Installationsverzeichnis>\sessionserver\sdk\javascript` verfügbar.

> **Hinweis**
>
> Das SameSite-Flag muss bei Verwendung der JavaScript-API angepasst werden. Siehe Festlegen des SameSite-Attributs.

6.5 Erweitern des Webclients

Sie können die Darstellung des Webclients mit eigenem HTML-, CSS- oder JavaScript-Code über den Browser aktualisieren, bearbeiten und anpassen.

Mit Erweiterungen können Sie optische Änderungen am Webclient vornehmen und die Anwendung anpassen. Der Webclient hostet den benutzerdefinierten HTML- oder CSS-Code, sodass er sich einfach ändern und pflegen lässt.

Weitere Informationen:

- Hinzufügen einer Erweiterung
- Erweiterungsbeispiel

6.5.1 Hinzufügen einer Erweiterung

Beachten Sie vor dem Fortfahren, dass Host Access for the Cloud zwar die Möglichkeit zum Planen und Verwenden von benutzerdefiniertem Code bietet, der Code selbst aber von den Entwicklern gepflegt werden muss, die ihn erstellt haben.

> **Achtung**
>
> Bei einer Produktaufrüstung werden die Erweiterungen deaktiviert. Das bedeutet, dass Sie nach einer Aufrüstung überprüfen müssen, ob das Produkt ohne die Erweiterungen wie erwartet funktioniert, und die Erweiterungen dann gemäß den Schritten zum Hinzufügen von benutzerdefiniertem Code erneut aktivieren müssen.

Wenn Sie Erweiterungen zum Webclient hinzufügen, sind die Änderungen für alle Benutzer sichtbar und werden auf alle Sitzungen angewendet.

So fügen Sie eine Erweiterung hinzu:

1. Öffnen Sie die Datei `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/service.yml`.
2. Fügen Sie „extensions_enabled“ an den vorhandenen Wert der Eigenschaft SPRING_PROFILES_ACTIVE an. Trennen Sie Werte mit einem Komma.

   Beispiel:

   ```
   env:
     - name: SPRING_PROFILES_ACTIVE
       value: tls,extensions_enabled
   ```

3. Starten Sie den Sitzungsserver neu.
4. Erstellen Sie die Datei `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/extensions/client/index.html` als Einstiegspunkt. Hier fügen Sie den HTML-, CSS- oder JavaScript-Code hinzu (einschließlich Verweise auf externe Skripte).

Bereitstellen von Erweiterungen ohne Clientauthentifizierung

Dateien im Verzeichnis `/client` sind mit der in MSS ausgewählten Authentifizierungsebene geschützt.

So geben Sie Dateien frei, ohne dass eine Authentifizierung erforderlich wird:

Erstellen Sie `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/extensions/public/`. Platzieren Sie Ihren Code in dieses Verzeichnis und rufen Sie ihn mithilfe der URL `/public/*` auf.

6.5.2 Erweiterungsbeispiel

In diesem Beispiel wird nach dem Aktivieren der Erweiterungen (siehe Schritt 2 oben) benutzerdefinierter CSS- und JavaScript-Code hinzugefügt, um die Schriftfarbe der Menübeschriftung zu ändern und Text zur JavaScript-Konsole auszugeben.

Sie erstellen drei Dateien: `custom.css`, `custom.js` und `index.html`.

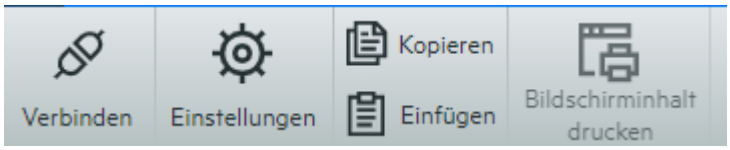
Schritt 1

Suchen Sie die in Schritt 4 oben erstellte Datei `index.html`. Hier legen Sie die Erweiterungsdateien ab und erstellen einen Einstiegspunkt:

```
<!-- Link zum externen Stylesheet definieren -->
<link href="client/custom.css" rel="stylesheet">
<!-- Externe JavaScript-Datei definieren -->
<script src="client/custom.js"></script>
```

Schritt 2

Ändern Sie die standardmäßig schwarze Menübeschriftung in orange:



Erstellen Sie „custom.css“, um die Farbe in orange zu ändern:

```
/* Linktext orange darstellen */
a span {
color: #ff5d28;
}
```

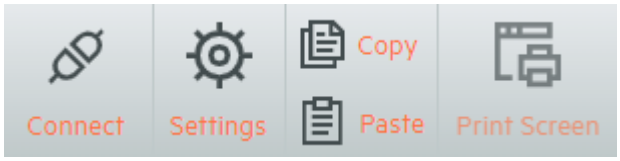
Schritt 3

Erstellen Sie „custom.js“, um Text zur JavaScript-Konsole zu senden:

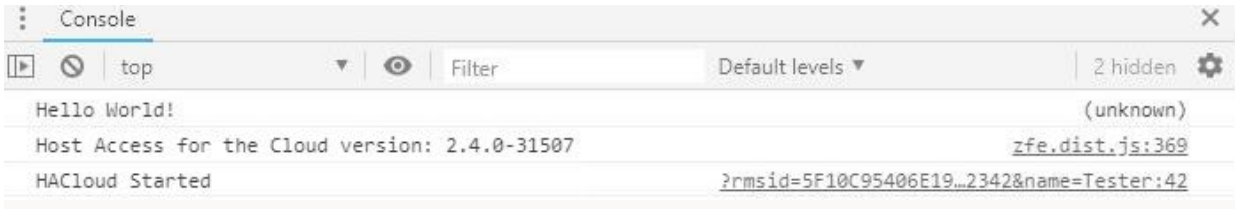
```
//Nachricht zur JavaScript-Konsole drucken
console.log('Hello World!');
```

Schritt 4

Nachdem die Dateien eingerichtet wurden (`<Installationsverzeichnis>/sessionserver/microservices/sessionserver/extensions/client/index.html`), sollte das Ergebnis folgendermaßen aussehen:



Außerdem wird der Text „Hello World“ in der JavaScript-Konsole angezeigt:



Weitere Informationen:

HACloud-API-Dokumentation

7. Technische Referenzen

7.1 Technische Referenzen

In diesem Kapitel finden Sie Informationen zu spezifischen Problemen, die unter Umständen auftreten können. Im Handbuch zum technischen Support von Micro Focus finden Sie Informationen dazu, wie Sie technischen Support für Ihr Produkt erhalten, auf unsere Onlineressourcen zugreifen und unseren technischen Support weltweit kontaktieren und nutzen.

7.2 Überwachen der Sitzungssserver mit Prometheus und Grafana

Sie können Host Access for the Cloud-Sitzungsserver mit Prometheus und Grafana überwachen. Beide Werkzeuge sind kostenlose Open-Source-Lösungen und können in Docker-Containern ausgeführt werden, was eine einfache Bereitstellung ermöglihcht. Jeder Sitzungsserver stellt einen Prometheus-Endpunkt bereit, der Metriken zum Server präsentiert. Prometheus kann zum Analysieren von Daten von diesem Endgerät und fortwährenden Speichern dieser Daten, auch von mehreren Sitzungsservern, konfiguriert werden. Grafana stellt dann ein Dashboard bereit, mit dem die Daten mit nur wenigen Einrichtungsschritten abgerufen und grafisch dargestellt werden können.

Voraussetzungen:

Docker und Docker Compose müssen installiert sein.

Schritte:

1. Erstellen Sie eine Docker Compose-Datei (.yml), die Grafana- und Prometheus-Images enthält.
2. Verknüpfen Sie Prometheus mit dem Prometheus-Endpunkt des Sitzungsservers.
3. Konfigurieren Sie die Grafana-Datenquelle zur Kommunikation mit Prometheus und importieren Sie die vorkonfigurierten Dashboards.
4. Grafana-Dashboards konfigurieren.
5. Greifen Sie auf Grafana zu.

7.2.1 Schritt 1. Docker Compose-Datei erstellen

Erstellen Sie die Datei `docker-compose.yml` mit Grafana- und Prometheus-Images.

```
version: "3.1"
services:
  grafana:
    build: grafana
    ports:
      - '3000:3000'
  prometheus:
    image: prom/prometheus:v2.6.1
    ports:
      - '9090:9090'
    volumes:
      - ./config/prometheus.yml:/etc/prometheus/prometheus.yml
      - ./prometheus:/prometheus
    networks:
      monitoring:
        aliases:
          - prometheus
networks:
  monitoring:
```

7.2.2 Schritt 2. Prometheus mit dem Prometheus-Endgerät von HACloud verknüpfen

Um Prometheus mit dem Endgerät zu verknüpfen, generieren Sie eine Datei `prometheus.yml`.

- In diesem Beispiel wird die Datei `prometheus.yml` im Konfigurationsverzeichnis gespeichert.
- Diese Beispielkonfiguration ermöglicht das Analysieren von Daten vom Prometheus-Endgerät mit HTTP oder HTTPS (TLS).
- Falls TLS auf dem Sitzungsserver deaktiviert ist, entfernen Sie tls_config und ändern Sie das Schema in der Beispielkonfiguration zu http.
- Konfigurieren Sie session-server-hostname (den Hostnamen des Sitzungsservers).

> **Hinweis**
>
> Aufgrund des Docker-Networking muss dies die eigentliche IP-Adresse oder der Hostname des Sitzungsserver-Hostcomputers sein. Diese IP-Adresse kann üblicherweise mit ifconfig/ipconfig abgerufen werden.

- Passen Sie die Ports je nach Bedarf an.

Beispiel: config/prometheus.yml

```
scrape_configs:
  - job_name: ' HACloud-Sitzungsserver mit TLS'
    scrape_interval: 15s
    scheme: https
    tls_config:
      insecure_skip_verify: true
    metrics_path: actuator/prometheus
    static_configs:
      - targets: ['session-server-hostname:7443']
```

7.2.3 Schritt 3. Kommunikation zwischen Prometheus und der Datenquelle konfigurieren

Die Kommunikation zwischen der lokalen Instanz von Prometheus und der Grafana-Datenquelle kann im Grafana-Docker-Image konfiguriert werden. Vorab geladene Dashbaords sind beim Starten verfügbar.

Beispiel: grafana/Dockerfile

```
FROM grafana/grafana:8.0.5
ADD ./provisioning /etc/grafana/provisioning
ADD ./config.ini /etc/grafana/config.ini
ADD ./dashboards /var/lib/grafana/dashboards
```

Beispiel: grafana/config.ini

```
[paths]
provisioning = /etc/grafana/provisioning
```

Beispiel: grafana/provisioning/datasources/all.yml

```
datasources:
- name: 'Prometheus'
  type: 'prometheus'
  access: 'browser'
  url: 'http://localhost:9090'
```

```
  is_default: true
  editable: false
```

Beispiel: grafana/provisioning/dashboards/all.yml

```
- name: 'default'
  org_id: 1
  folder: ''
  type: 'file'
  options:
    folder: '/var/lib/grafana/dashboards'
```

7.2.4 Schritt 4. Grafana-Dashboards konfigurieren

Die JSON-Beispieldatei hilft Ihnen beim Einstieg in die Konfiguration Ihrer Grafana-Dashboards.

So sorgen Sie dafür, dass Ihr Docker-Container das Dashboard beim Start lädt:

- Suchen Sie `HACloudSessionservers.json` im Verzeichnis `hacloud/utilities/grafana`.
- Kopieren Sie `HACloudSessionservers.json` in Ihr Verzeichnis `grafana/dashboards`.

7.2.5 Schritt 5. Auf Grafana zugreifen

- Starten Sie den Docker-Container mit dem Befehl docker-compose up -d.
- Überprüfen Sie mit `http://localhost:9090/targets`, ob die Prometheus-Ziele die Sitzungsserver erfolgreich analysieren.
- Greifen Sie mit `http://localhost:3000` auf Grafana zu.
- Benutzername und Passwort lauten *admin*. Der Benutzername und das Passwort können in mit Docker-Umgebungsvariablen konfiguriert werden.
- Stoppen Sie den Docker-Container mit dem Befehl docker-compose down .

7.3 Ausführen des Sitzungsserverdiensts als dedizierter Benutzer mit eingeschränkten Berechtigungen

Aus Sicherheitsgründen sollten Sie den Sitzungsserverdienst als dedizierter Benutzer mit eingeschränkten Berechtigungen ausführen.

> **Hinweis**
>
> Sie müssen diese Schritte nach jeder Produktaufrüstung wiederholen.

Vorgehensweise auf einer Windows-Plattform:

1. Erstellen Sie nach der ersten Installation des Produkts einen Standardbenutzer.
2. Gewähren Sie dem Benutzer Vollzugriff auf die folgenden Verzeichnisse:
   - `<Installationsverzeichnis>\sessionserver\logs`
   - `<Installationsverzeichnis>\sessionserver\tmp`
3. Beenden Sie im Dialogfeld der Windows-Dienste den Dienst für den Micro Focus Host Access for the Cloud-Sitzungsserver.
4. Öffnen Sie die Eigenschaften des Host Access for the Cloud-Sitzungsserverdiensts.
5. Öffnen Sie die Registerkarte zur Anmeldung und wählen Sie **Dieses Konto** aus.
6. Geben Sie den Benutzernamen und das Kennwort des Benutzers ein, der den Dienst ausführen soll.
7. Starten Sie den Sitzungsserverdienst.

Vorgehensweise auf Unix/Linux:

Führen Sie die oben genannten Schritte aus, passen Sie sie jedoch entsprechend für Ihre Umgebung und Verteilung an.

Weitere Informationen

Running the Micro Focus MSS Server service as a dedicated user (Ausführen des Micro Focus MSS-Serverdiensts als dedizierter Benutzer)

7.4 Festlegen des SameSite-Attributs

Um websiteübergreifende Anforderungsfälschungen zu verhindern, wurde das standardmäßige SameSite-Attribut im Sitzungsservercookie von **None** („Keine“, weniger streng) auf **Lax** (strenger) aktualisiert.

Wenn das Attribut auf „Lax“ festgelegt ist, wird das Sitzungsservercookie nicht bei siteübergreifenden Anforderungen gesendet, wie dies häufig beim JavaScript-SDK und bei der SAML-Authentifizierung der Fall ist.

Diese Änderung betrifft zwei Bereiche von HACloud:

- das JavaScript-SDK
- die SAML-Authentifizierung hinter einem Lastverteiler

In diesen Fällen müssen Sie den Attributwert auf **None** (Keine) festlegen, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie `container.properties` in einem Texteditor. Das Standardverzeichnis für diese Datei ist `./sessionserver/conf/`.
2. Fügen Sie die folgende Zeile zu `container.properties` hinzu:

   `samesite.cookie.attribute=None`
3. Starten Sie den Sitzungsserver neu.

7.5 Ändern des Größenlimits für das Hochladen bei Dateiübertragungen

Für Dateiübertragungen gilt beim Hochladen ein Dateigrößenlimit von 50 MB. Um das Dateigrößenlimit zu ändern, legen Sie `spring.servlet.multipart.maxfilesize` und `spring.servlet.multipart.maxrequestsize` in `HACloud/sessionserver/microservices/sessionserver/service.yml` wie gewünscht fest und starten Sie den Sitzungsserver neu.

Beispiel:

```
- name: spring.servlet.multipart.maxfilesize
  value: "100MB"
- name: spring.servlet.multipart.maxrequestsize
  value: "100MB"
```

7.6 Konfigurieren der MSS-Callback-Adresse

MSS stellt dem Sitzungsserver bei jedem Erstellen oder Bearbeiten einer Sitzung eine Callback-Adresse bereit.

Standardmäßig wird die in `management.server.url` angegebene Adresse verwendet.

Wenn sich der MSS-Server hinter einem Proxy befindet und der Sitzungsserver die Adresse nicht erreichen kann:

- Legen Sie die Eigenschaft `management.server.callback.address` in jeder MSS-Datei „container.properties“ auf eine Adresse fest, die der Sitzungsserver für eine bestimmte MSS-Instanz erreichen kann.
- Starten Sie den Server neu, um die neuen Eigenschaftswerte zu übernehmen.

7.7 Kopieren von Sitzungen zwischen Management and Security Server-Instanzen

Sie können Reflection for the Web-Sitzungen kopieren und konvertieren und für einen andere Instanz von Management and Security Server (MSS) und Host Access for the Cloud verfügbar machen.

> **Hinweis**
>
> In den folgenden Schritten ist die Management and Security Server-Instanz, von der Sie Sitzungen kopieren, die **Quelle** und die Management and Security Server-Instanz, zu der Sie sie kopieren, das **Ziel**.

Führen Sie die folgenden Schritte aus, um Sitzungen vom Quellserver zum Zielserver zu kopieren:

1. Stoppen Sie den MSS-Zielserver.
2. Öffnen Sie auf dem MSS-Quellserver sowie auf dem MSS-Zielserver die Datei „SessionDS.xml“ im folgenden Verzeichnis:
   - Unter Windows: `C:\ProgramData\Micro Focus\MSS\MSSData`
   - Unter Linux: `/var/opt/microfocus/mss/mssdata`
3. Suchen Sie in der XML-Quelldatei das OBJECT_ARRAY-Element.
4. Suchen und kopieren Sie in der XML-Quelldatei unter OBJECT_ARRAY die untergeordneten Sitzungselemente von Reflection for the Web.
5. Öffnen Sie die XML-Zieldatei, und fügen Sie sie unter dem OBJECT_ARRAY-Element der Zieldatei ein.
6. Suchen Sie in der Zieldatei das OBJECT_ARRAY-Größenattribut, das der Anzahl der Sitzungen entspricht. Erhöhen Sie diesen Wert um die Anzahl der hinzugefügten Sitzungselemente. Wenn Sie beispielsweise sechs Sitzungselemente in der Zieldatei eingefügt haben und der Wert des vorhandenen OBJECT_ARRAY-Größenattributs auf 4 festgelegt ist, müssen Sie den Wert um 6 erhöhen. Das Größenattribut muss dann den Wert 10 aufweisen. Unter dem OBJECT_ARRAY-Element sind nun 10 Sitzungselemente aufgeführt.
7. Sitzungsnamen müssen eindeutig sein. Prüfen Sie die Zieldatei auf doppelte Sitzungsnamen. Die Sitzungsnamen finden Sie im untergeordneten Sitzungselement „SessionName“.
8. Kopieren Sie die Konfigurationsdateien für jede Sitzung, die in „SessionDS.xml“ hinzugefügt wurde, vom Quell- auf den Zielserver. Die Namen der Konfigurationsdateien finden Sie unter dem Sitzungselement im untergeordneten Element „configuration“. Die Dateien selbst befinden sich im folgenden Verzeichnis:
   - Unter Windows: `C:\ProgramData\Micro Focus\MSS\MSSData\deploy\dyncfgs`
   - Unter Linux: `/var/opt/microfocus/mss/mssdata/deploy/dyncfgs`
9. Starten Sie den MSS-Zielserver neu. Öffnen Sie die Verwaltungskonsole. In der Liste „Manage Sessions“ (Sitzungen verwalten) sollten alle kopierten Reflection for the Web-Sitzungen angezeigt werden.
10. Im nächsten Schritt wird die Reflection for the Web-Sitzung in eine Host Access for the Cloud-Sitzung konvertiert. Klicken Sie in „Manage Sessions“ (Sitzungen verwalten) mit der rechten Maustaste auf die Sitzung, die konvertiert werden soll. Sitzungstypen werden durch ein Symbol in der Spalte „Typ“ identifiziert.
11. Informationen zum Konvertieren einer Reflection for the Web-Sitzung in eine Host Access for the Cloud-Sitzung in der Verwaltungskonsole finden Sie unter Convert a Reflection for the Web session (Konvertieren einer Reflection for the Web-Sitzung).

7.8 Ändern der Ports

Eine Liste der standardmäßigen Ports, die von Host Access for the Cloud verwendet werden, finden Sie unter „Ports“.

So ändern Sie die Standardports:

Komponente	Anweisungen
Host Access for the Cloud-Sitzungsserver	Öffnen Sie `sessionserver/microservices/sessionserver/service.yml`, um Folgendes zu ändern: `-name : SERVER_PORT` und `value: "7443"`
Management and Security Server	Der von MSS für die Herstellung einer HTTPS-Verbindung verwendete SSL-Port ist standardmäßig auf 443 gesetzt. Starten Sie Management Server, wenn Sie die Portnummer ändern müssen. Dadurch wird die Standarddatei PropertyDS.xml erstellt. Öffnen Sie anschließend im Verzeichnis „MssData“ die Datei „PropertyDS.xml“. Ändern Sie im nachfolgenden Abschnitt den Wert von 443 in die entsprechende Portnummer und starten Sie dann Management Server neu. `<CORE_PROPERTY NAME="sslport"> <STRING>443</STRING>`

7.9 Automatisches Starten und Beenden von Diensten

Alle Serverkomponenten werden als Dienste installiert und können während der Installation für den Start konfiguriert werden.

Wenn Sie auf Linux-Plattformen arbeiten, führen Sie die nachstehenden Schritte aus, um den Sitzungsserver so einzurichten, dass er beim Systemstart automatisch gestartet wird.

Erstellen Sie mithilfe Ihres Installationsverzeichnisses eine Datei mit der Bezeichnung `sessionserver` und dem folgenden Inhalt:

```
#!/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=<enter installation directory>
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
```

Führen Sie dann die jeweils relevanten Schritte aus.

Unter Linux:

1. Kopieren Sie die Datei in das Verzeichnis `/etc/init.d`.
2. Legen Sie die Dateiberechtigungen fest. Führen Sie unter Verwendung des Werts 755 den Befehl `chmod` aus. Beispiel: `chmod 755 sessionserver`
3. Führen Sie `chkconfig` aus, um das Initialisierungsskript hinzuzufügen. Beispiel: `/sbin/chkconfig --add sessionserver`

7.10 URL-Pfad des Sitzungsservers anpassen

Sie können den URL-Pfad für den Zugriff auf den Sitzungsserver anpassen.

Beispielsweise können Sie `https://meinserver:7443/` zu `https://meinserver.com:7443/hacloud/` ändern.

1. Öffnen Sie die Datei `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/service.yml`.
2. Fügen Sie den folgenden Eintrag (ohne Formatierungsänderungen) hinzu und ersetzen Sie *Pfad* durch den von Ihnen gewünschten Wert.

```
- name: SERVER_SERVLET_CONTEXTPATH
  value: "/<Pfad>"
```

3. Starten Sie den Sitzungsserver neu.
4. Unter `https://<Sitzungsserver>:7443/<angegebener Pfad>/` können Sie auf Ihren Sitzungsserver zugreifen.

7.11 Konfigurieren von Benutzernamen bei Verwendung der anonymen Zugangssteuerung

Benutzer benötigen Zugriff auf ihre Makros, Benutzerkonfigurationen und andere personalisierte Einstellungen, unabhängig davon, ob sie über Management and Security Server authentifiziert sind oder nicht. Diese Einstellungen werden gesammelt als „Benutzereinstellungen“ bezeichnet.

Wenn MSS zur Authentifizierung beispielsweise mit LDAP oder SAML konfiguriert ist, wird beim Anmelden des Benutzers ein Benutzername ermittelt. Die Einstellungen des Benutzers werden zentral in MSS gespeichert und der ermittelte Benutzername wird für alle zukünftigen Anmeldungen verwendet.

Wenn jedoch die MSS-Authentifizierungsmethode auf „Keine“ festgelegt ist, was auch als anonymer Modus bezeichnet wird, steht dem System kein eindeutiger Benutzername zur Verfügung, anhand dem der Benutzer bei späteren Anmeldungen identifiziert werden könnte. In dieser Konfiguration teilen alle Benutzer die gleichen Einstellungen. Wenn ein Benutzer eine Einstellung ändert, wird diese Einstellung auch für alle anderen Benutzer geändert.

Da dies nicht immer dem gewünschten Verhalten entspricht, unterstützt Host Access for the Cloud mehrere Möglichkeiten, mit denen der Administrator eine eindeutige Kennung für jeden Benutzer konfigurieren kann, damit benutzerdefinierte Einstellungen gespeichert und für spätere Anmeldungen abgerufen werden können.

> **Hinweis**
>
> Diese Konfigurationsänderungen wirken sich nicht auf die Sicherheitsüberlegungen zur Verwendung von Management and Security Server im anonymen Modus aus.

7.11.1 Konfigurationsoptionen

Beim Konfigurieren von Kennungen für Benutzernamen können Sie eine von vier verschiedenen Konfigurationsoptionen auswählen. Sie müssen den Sitzungsserver neu starten, damit Änderungen wirksam werden.

- So verwenden Sie einen HTTP-Anforderungscookiewert als Benutzernamen

  Fügen Sie die folgenden Zeilen zu `<Sitzungsserver>/conf/container.properties` hinzu:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.CookieKeyAnonymousPrinci
  zfe.principal.name.identifier=<zu-verwendendes-Cookie>
  ```

- So verwenden Sie einen HTTP-Anforderungsheaderwert als Benutzernamen

  Fügen Sie die folgenden Zeilen zu `<Sitzungsserver>/conf/container.properties` hinzu:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.HeaderKeyAnonymousPrinci
  zfe.principal.name.identifier=<zu-verwendender-Header>
  ```

- So verwenden Sie einen HTTP-Anforderungs-URL-Parameter als Benutzernamen

  Fügen Sie die folgenden Zeilen zu `<Sitzungsserver>/conf/container.properties` hinzu:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.UrlParameterAnonymousPri
  zfe.principal.name.identifier=<zu-verwendender-URL-Parameter>
  ```

- So verwenden Sie die IP-Adresse des Clients als Benutzernamen

  Fügen Sie die folgende Zeile zu `<Sitzungsserver>/conf/container.properties` hinzu:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.RemoteAddrAnonymousPrinc
  ```

7.11.2 Beheben von Fehlern mit der Konfiguration

Wenn bei Benutzern Probleme beim Herstellen der Verbindung mit einer Host Access for the Cloud-Webanwendung auftreten, nachdem Sie die Konfigurationsänderungen vorgenommen haben, sollten Sie Folgendes überprüfen:

- Benutzer erhalten die Meldung *503 Service Unavailable*(Service nicht verfügbar), wenn sie versuchen, eine Verbindung zu einer Host Access for the Cloud-Webanwendung herzustellen. Prüfen Sie zunächst die Protokolldatei (`<Sitzungsserver>/logs/sessionserver.log`) und gehen Sie dann wie folgt vor:
  - Wenn die Protokolldatei die Meldung *Unable to create AnonymousPrincipalNameProvider instance for class...* (AnonymousPrincipalNameProvider-Instanz kann nicht erstellt werden für Klasse...) enthält, wurde die Eigenschaft `zfe.principal.name.provider` vermutlich falsch eingegeben. Überprüfen Sie die Rechtschreibung und die Groß- und Kleinschreibung, um dieses Problem zu beheben.
  - Wenn die Protokolldatei die Meldung *zfe.principal.name.identifier is not defined* (zfe.principal.name.identifier ist nicht definiert) enthält, ist die Eigenschaft nicht vorhanden. Stellen Sie sicher, dass die Eigenschaft definiert ist, um das Problem zu beheben.
- Benutzer können sich nicht ordnungsgemäß authentifizieren.

  Die Benutzer sollten eine Fehlermeldung darüber erhalten, dass die anfängliche HTTP-Anforderung an die Host Access for the Cloud-Webanwendung nicht die erforderlichen Informationen enthielt.

7.12 Zugriff auf Host Access for the Cloud mit IIS-Reverseproxy

Dieser Abschnitt erläutert die Verwendung von IIS-Reverseproxy mit Host Access for the Cloud. Um die Common Criteria-Sicherheitsanforderungen zu erfüllen, muss der Host Access for the Cloud-Server auf nachfolgende Weise hinter einem Proxy platziert werden.

Voraussetzungen

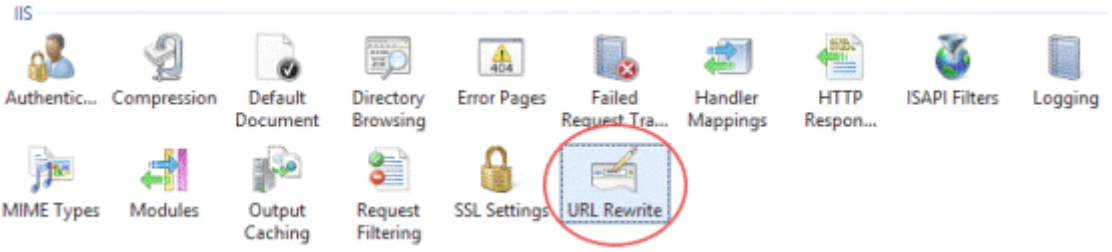
- Internet Information Services (IIS) 8.0 oder höher muss installiert sein.
- Das IIS-WebSockets-Protokoll muss aktiviert sein. Informationen zum Aktivieren dieses Protokolls finden Sie unter IIS 8.0 WebSocket Protocol Support (Unterstützung des WebSocket-Protokolls in IIS 8.0).
- IIS Application Request Routing (ARR) 3.0 oder höher ist erforderlich.
- Das IIS-URL-Rewrite-Modul muss installiert sein.

7.12.1 Konfigurieren des IIS-Reverseproxys für HACloud

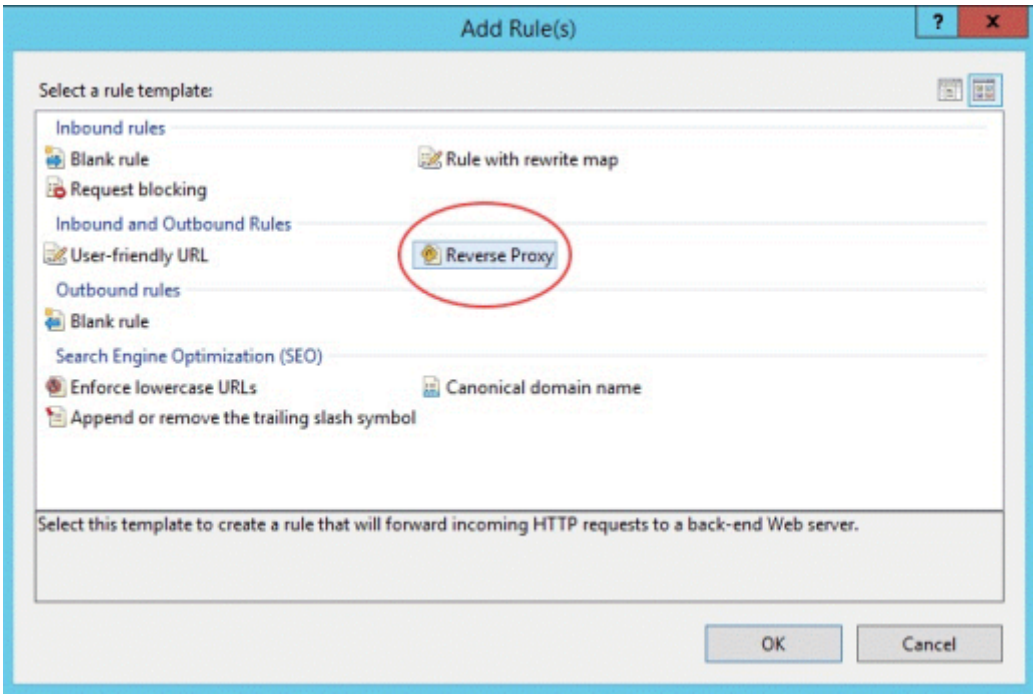
In diesem Beispiel wird die Konfiguration eines IIS-Servers mit der IP-Adresse 192.168.1.1 für Proxyverbindungen zum Host Access for the Cloud-Sitzungsserver unter `http://10.10.10.1:7070` veranschaulicht.

IIS konfigurieren

1. Starten Sie den Internet Information Services-Manager (IIS-Manager), navigieren Sie zu der zu verwendenden Website und öffnen Sie die URL-Rewrite-Funktion.



2. Wählen Sie die Aktion „Regel hinzufügen“ aus und fügen Sie die Reverseproxy-Regel hinzu.



3. Geben Sie für die eingehende Regel den Hostnamen oder die IP-Adresse und den Port des Host Access for the Cloud-Servers ein. Wenn der Host Access for the Cloud-Sitzungsserver beispielsweise auf dem gleichen Computer installiert ist wie IIS und der zugehörige Standardport verwendet wird, geben Sie `localhost:7443` ein.
4. Aktivieren Sie die ausgehende Regel „Rewrite the domain names...“ (Domänennamen umschreiben) und geben Sie den Hostnamen oder die IP-Adresse des IIS-Servers im Feld „To:“ (An) ein.
5. Klicken Sie auf „OK“, um die neue Reverseproxy-Regel zu erstellen.

HACloud konfigurieren

Zum Herstellen von Proxyverbindungen muss das IIS-URL-Rewrite-Modul die Webseiten und WebSocket-Verbindungen, die den Proxy durchlaufen, prüfen und umschreiben. Zur erfolgreichen Umschreibung müssen diese Elemente in nicht komprimierter Form gesendet werden. Beachten Sie, dass die konfigurierte Komprimierung weiterhin vom IIS-Server zum Browser des Clients

erfolgt. Der Sitzungsserver muss auch so konfiguriert werden, dass WebSocket-Verbindungen vom Proxy ausgehen können.

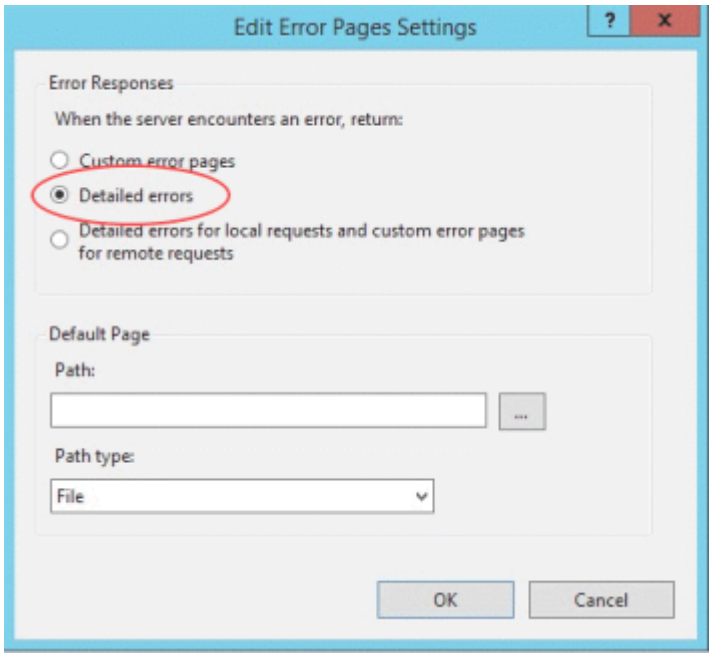
1. Öffnen Sie „container.properties“ in einem Texteditor. Der Standardspeicherort für diese Datei ist: /sessionserver/conf.
2. Fügen Sie die folgenden Zeilen zu `container.properties` hinzu:

```
websocket.compression.enable=false
server.compression.enabled=false
websocket.allowed.origins=http://<Name oder IP-Adresse des IIS-Servers>. Beispiel: 192.168.1.1.
```

   Speichern Sie die Änderungen in der Datei. Die Eigenschaft „Zulässige Ursprünge“ ist eine durch Kommas getrennte Liste von URLs. Wenn Webclients über HTTPS eine Verbindung mit Ihrer Website herstellen, passen Sie die URL entsprechend an. Wenn sichere sowie nicht sichere Verbindungen verwendet werden, verwenden Sie beide URLs als Wert: `websocket.allowed.origins=http://192.168.1.1,https://192.168.1.1` . Um Fehler zu vermeiden, sollten Sie sicherstellen, dass in der Liste „Zulässige Ursprünge“ alle möglichen Adressformate enthalten sind.
3. Starten Sie die Website und den Sitzungsserver neu und testen Sie den Proxy durch Herstellen einer Verbindung mit `http(s)://192.168.1.1` .

Fehlersuche

Wenn Webserverfehler ausgegeben werden, kann das Problem durch Aktivieren der detaillierten Fehler diagnostiziert werden. Öffnen Sie im IIS-Manager die Funktion „Fehlerseiten“ und aktivieren Sie „Detaillierte Fehler“:



Normalerweise werden Fehler im 5XX-Bereich durch Probleme mit der aktivierten Komprimierung oder Fehler im Wert „Zulässige Ursprünge“ verursacht.

Wenn der IIS-Proxy über HTTPS eine Verbindung mit dem Sitzungsserver herstellt, muss das mit dem Sitzungsserver verwendete Zertifikat vom IIS-Server verbürgt werden. Wenn der Sitzungsserver ein eigensigniertes Zertifikat verwendet, muss dieses Zertifikat zum Windows-Truststore hinzugefügt werden. Wenn der Sitzungsserver ein signiertes Zertifikat verwendet, muss der Signaturgeber eine vertrauenswürdige Zertifizierungsstelle sein.

7.13 Verwendung von IIS-Reverseproxy mit Host Access for the Cloud

Um die Common Criteria-Sicherheitsanforderungen zu erfüllen, muss der Sitzungsserver möglicherweise hinter einem Proxy platziert werden. Lesen Sie vor dem Konfigurieren die Informationen zu Voraussetzungen und die Konfigurationsanweisungen im Abschnitt „Zugriff auf Host Access for the Cloud mit IIS-Reverseproxy“.

> **Hinweis**
>
> Zur Erfüllung der Common Criteria-Sicherheitsanforderungen kann es erforderlich sein, den Sitzungsserver hinter einem Proxy zu platzieren. Befolgen Sie hierzu die Anweisungen unter „Zugriff auf Host Access for the Cloud mit IIS-Reverseproxy“.

Wenn Sie über IIS eine Proxyverbindung für Host Access for the Cloud herstellen möchten und IIS Single Sign-on verwenden, legen Sie in derselben container.properties-Datei eine weitere Eigenschaft fest:

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

Der Wert hat das gleiche Format wie die URL oben, verwendet aber die Host Access for the Cloud-Adresse. Beispiel: `http://server/`. Für diese URL ist es nicht erforderlich, eine Kurzform des Hostnamens zu verwenden.

Nachdem Sie diese Konfiguration abgeschlossen haben, wählen Sie in der Verwaltungskonsole von Management and Security Server unter „Assign Access“ (Zugriff zuweisen) diese Authentifizierungsoption aus. Beschreibungen der Konfigurationsoptionen finden Sie in der Onlinehilfe der Verwaltungskonsole.

Weitere Informationen:

- Single Sign-on über IIS konfigurieren

7.14 Konfigurieren von Cross-Origin Resource Sharing (CORS)

Als Sicherheitsmaßnahme schränken moderne Webbrowser die Arten von Interaktionen ein, die zwischen verschiedenen Websites zulässig sind. Dies kann zu Problemen beim Versuch der standortübergreifenden Integration führen, z. B. beim Einbetten des HACloud-Webclients in eine andere Website wie ein Portal. CORS ist ein Standardmechanismus, mit dem Sie angeben können, dass der Browser den Zugriff von einer Site auf eine andere Website zulässt.

Durch Aktualisieren der Datei `service.yml` können Sie den HACloud-Sitzungsserver so konfigurieren, dass er den erforderlichen CORS-HTTP-Header einschließt, wenn er auf die Webanforderungen reagiert.

1. Öffnen Sie die Datei `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/service.yml`.
2. Fügen Sie Folgendes zur Datei hinzu:

```
    - name: CORS_ALLOWED_ORIGINS
      value: "https://integration-server1.com"
```

3. Starten Sie den Sitzungsserver neu.

Sie können diesen Wert auf eine durch Kommas getrennte Liste zulässiger Ursprünge festlegen oder den Platzhalter `*` verwenden, um den Zugriff von allen Ursprüngen aus zuzulassen (das Zulassen dieser Art von offenem Zugriff kann ein Sicherheitsrisiko darstellen). Wenn Sie die Platzhalteroption (*) verwenden, beachten Sie, dass Webbrowser zusätzliche Einschränkungen auferlegen, z. B. eingeschränkten Cookie-Zugriff. Weitere Informationen finden Sie unter Cross-Origin Resource Sharing (CORS) – HTTP/MDN.

7.15 Anpassen des HTTP-Sitzungstimeouts

Der standardmäßige Zeitüberschreitungswert für eine inaktive Benutzersitzung beträgt 30 Minuten. Das bedeutet: Jedes Mal, wenn ein Benutzer den Browser schließt, ohne sich zuvor abzumelden, werden sowohl die Benutzersitzung als auch jegliche offenen Hostsitzungen nach 30 Minuten bereinigt. Der zulässige Mindesttimeoutwert beträgt 600 Sekunden (10 Minuten). Sie können diese Einstellung auf dem Server konfigurieren.

1. Öffnen Sie die Datei `<Installationsverzeichnis>/sessionserver/microservices/sessionserver/service.yml`.
2. Passen Sie den Wert für die Sitzungszeitüberschreitung im Abschnitt `env` der Datei an:

```
- name: server.servlet.session.timeout
  value: <gewünschte Dauer in Sekunden>
```

> **Hinweis**
>
> Die Einzüge in der Formatierung müssen beibehalten werden.

3. Starten Sie den Server neu.

7.16 Aktivieren der FIPS-Sicherheit

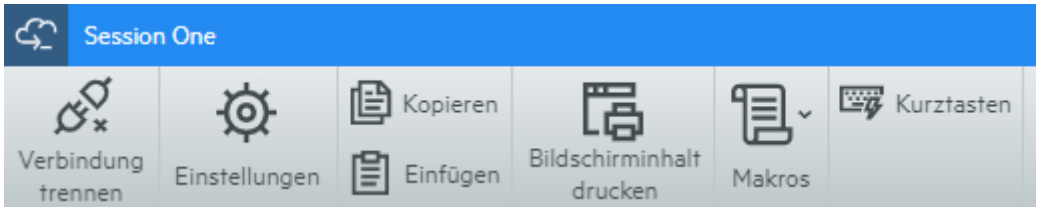
Die geprüften Verschlüsselungsmodule des Federal Information Processing Standard (FIPS) 140-2 werden von der US-Regierung als Standard für Sicherheitsbestimmungen verwendet. Host Access for the Cloud unterstützt diesen Standard. Sie können den FIPS-Modus einfach durch Bearbeiten einer Datei auf dem Sitzungsserver aktivieren.

- Öffnen Sie die Datei `<Installationsverzeichnis>\sessionserver\microservice\sessionserver\service.yml`.
- Fügen Sie das Flag `-Dcom.attachmate.integration.container.FIPS.enabled=true` zum Java-Befehl `start-command` hinzu.
- Starten Sie den Server neu.
- Um sicherzustellen, dass der FIPS-Modus aktiviert ist, öffnen Sie `<Installationsverzeichnis>\sessionserver\logs\sessionserver.log` und überprüfen Sie, ob der FIPS-Modus auf „true“ (wahr) festgelegt ist: `FIPS mode: true`.

7.17 Verwendung des Einzelsitzungsmodus

Sie können den Einzelsitzungsmodus verwenden und URLs für bestimmte Sitzungen angeben, die über namensspezifische Parameter gestartet werden (z. B. eine direkte Verbindung auf einer Unternehmensportalseite). Um den Start einer Einzelsitzung zu ermöglichen, verwenden Sie den Abfrageparameter „singleSession“. Sie können diesen Parameter allein verwenden, um nur den Webclient im Einzelsitzungsmodus zu starten, z. B. `http://<Sitzungsserver>:7443//?singleSession`. Alternativ kann der Parameter in Verbindung mit dem Parameter einer benannten Sitzung verwendet werden, um eine bestimmte benannte Sitzung im Einzelsitzungsmodus zu starten: `http://<Sitzungsserver>:7443//?singleSession&name=HumanResources`. Die Reihenfolge der Parameter spielt dabei keine Rolle.

Wenn die Benutzer auf eine Einzelsitzung zugreifen, können sie nicht zwischen geöffneten Sitzungen wechseln und keine neuen Sitzungen öffnen. Wenn die angegebene Sitzung beim Öffnen bereits vorhanden ist, wird keine neue Sitzung gestartet.



Wenn alle Sitzungen auf dem Sitzungsserver im Einzelsitzungsmodus ausgeführt werden sollen:

- Öffnen Sie `<Installationsverzeichnis>/sessionserver/conf/container.properties`.
- Fügen Sie `webclient.singleSession=true` zur Datei hinzu.

7.18 Bekannte Probleme

Folgende Probleme wurden in früheren Versionen identifiziert und sind bekannte Probleme.

Browserprobleme

Hostspezifische Probleme

Probleme bei der Installation

7.18.1 Browserprobleme

Die folgenden Hinweise beziehen sich auf verschiedene Webbrowser.

- Empfohlene Browser
- Probleme bei der Tastenbelegung in verschiedenen Browsern

Empfohlene Browser

Es wird dringend empfohlen, Google Chrome oder Mozilla Firefox zu verwenden. Host Access for the Cloud unterstützt Microsoft Internet Explorer (IE) 11. Es sind jedoch Leistungsprobleme mit dem JavaScript-Modul von Internet Explorer bekannt, die sich negativ auf das Endbenutzererlebnis mit Host Access for the Cloud auswirken können.

Diese Probleme wurden identifiziert und es gibt entsprechende Abhilfen. Die einfachste Lösung besteht jedoch darin, einen anderen Browser zu verwenden.

- Wiedergabe von aufgezeichneten Makros in Internet Explorer nicht möglich

  Bei Verwendung bestimmter älterer Versionen des Webbrowsers Microsoft Internet Explorer (IE) mit Host Access for the Cloud können bei der Wiedergabe von Makros Fehler auftreten. Folgende Fehlermeldung wird angezeigt: *Macro Error: Error transpiling macro code: TypeError: unknown: Circular reference in value argument not supported* (Makrofehler: Fehler beim Transpilieren des Makrocodes: TypeError: unbekannt: Zirkelbezug im Wertargument wird nicht unterstützt).

  Hierbei handelt es sich um ein Problem mit dieser Version von Internet Explorer und JavaScript. Dieser Fehler kann möglicherweise vermieden werden, wenn Sie die createMacro()-Funktion löschen und sie mit JavaScript Promises ersetzen (z. B. then()).

  Da dies ein spezifisches Problem bei früheren Versionen von Internet Explorer ist, besteht die einfachste Lösung darin, einen anderen Browser (Chrome oder Firefox) oder eine neuere Version von Internet Explorer zu verwenden. Makros können mit Internet Explorer Version 11.0.9600.18161, Updateversion 11.0.27 problemlos wiedergegeben werden. Führen Sie Windows Update aus, um Internet Explorer zu aktualisieren.

- HTTPS-Verbindungen zwischen mobilen Geräten unter Apple iOS und dem Sitzungsserver

  Benutzer von Host Access for the Cloud können bei Verwendung eines eigensignierten Zertifikats auf ihrem Apple iPad keine Verbindung mit einem Sitzungsserver über HTTPS herstellen. Sofern dies möglich ist, besteht die schnellste Lösung darin, HTTP anstelle von HTTPS zu verwenden.

  Wenn HTTPS erforderlich ist, haben Sie die folgenden Möglichkeiten:

  - Rufen Sie ein gültiges von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat ab, und installieren Sie es auf dem Sitzungsserver.
  - Verwenden Sie einen anderen Browser, in dem das selbstsignierte Zertifikat akzeptiert wird. Eine Liste der unterstützten Browser finden Sie unter „Unterstützung für Browser und Betriebssystem“.
  - Nutzen Sie eine benutzerdefinierte Zertifizierungsstelle:
    - Erstellen Sie eine benutzerdefinierte Zertifizierungsstelle, ein Zertifizierungsstellen-Stammzertifikat und ein durch das Stammzertifikat dieser Zertifizierungsstelle signiertes Serverzertifikat.
    - Installieren Sie das Serverzertifikat auf dem Sitzungsserver.
    - Installieren Sie das benutzerdefinierte Zertifizierungsstellen-Stammzertifikat über ein Profil auf dem iPad. Das Serverzertifikat sollte dann auf dem iPad akzeptiert werden, da es von einer „vertrauenswürdigen Zertifizierungsstelle“ signiert wurde.

  Eine Liste der vertrauenswürdigen Zertifizierungsstellen unter Apple iOS finden Sie unter Listen verfügbarer vertrauenswürdiger Root-Zertifikate in iOS.

- In Internet Explorer werden leere Bildschirme angezeigt

Bei Verwendung des Webbrowsers Microsoft Internet Explorer (IE) mit Host Access for the Cloud oder Management and Security Server (MSS) wird anstelle der erwarteten Sitzung möglicherweise ein leerer Bildschirm angezeigt.

Wenn mit Microsoft Internet Explorer auf Host Access for the Cloud-Sitzungen oder auf Management and Security Server zugegriffen wird, können Probleme der folgenden Art auftreten:

Host Access for the Cloud rendert für bestimmte URLs ordnungsgemäß und zeigt für andere einen leeren Bildschirm an. Das Verhalten variiert je nachdem, ob für die Sitzung eine IP-Adresse, ein kurzer Hostname oder ein vollqualifizierter Name verwendet wird.

In MSS kann eine Host Access for the Cloud-Sitzung nur erstellt oder geöffnet werden, wenn sie auf demselben Server ausgeführt wird wie MSS. Andernfalls wird anstelle der erwarteten Sitzung ein leerer Bildschirm angezeigt.

Erklärung

Dieses Problem ist spezifisch für die Weise, wie in Internet Explorer verschiedene Einstellungen entsprechend der Interpretation der Websitesicherheit umgeschaltet werden. Dies betrifft die Einstellungen „Kompatibilitätsansicht“ und „Cookies von Drittanbietern“. Abhängig davon, welche „Zone“ in Internet Explorer für Ihre Website ermittelt werden, müssen diese Einstellungen entweder aktiviert oder deaktiviert sein. Internet Explorer basiert die Bestimmung auf der URL der Website. Wenn der Servername in der URL beispielsweise keine Punkte enthält (z. B. `http://mycorporateserver/mss/AdminStart.html`), geht Internet Explorer davon aus, dass die Adresse zur Zone „Lokales Intranet“ gehört. Wenn dies der Fall ist, wird die Website der Zone „Internet“ zugewiesen.

Lokales Intranet

- Kompatibilitätsansicht aktiviert (nicht gewünscht)
- Cookies von Drittanbietern aktiviert (gewünscht)

Internet

- Kompatibilitätsansicht deaktiviert (gewünscht)
- Cookies von Drittanbietern deaktiviert (nicht gewünscht)

Zwar kann eine Website die Kompatibilitätsansicht durch Angabe des Dokumentmodus mit dem HTML-Metatag „X-UA-Compatible“ überschreiben und Host Access for the Cloud dann diesen spezifischen Modus verwenden, MSS verwendet diesen Modus aber nicht. Wenn also ein Host Access for the Cloud-Server und eine Management and Security Server-Instanz sich beide in der Zone „Lokales Intranet“ befinden (standardmäßig mit aktivierter Option „Kompatibilitätsansicht“) ist es wahrscheinlich, dass Host Access for the Cloud weiterhin ordnungsgemäß ausgeführt wird, MSS dagegen jedoch nicht.

Lösung

Zur Verwendung von Internet Explorer 10 oder 11 mit Host Access for the Cloud- und MSS-Servern sind folgende Einstellungen erforderlich:

Sie müssen bestimmen, in welcher Zone sich Ihre Website befindet, und dann die erforderlichen Anpassungen an den Einstellungen von Internet Explorer vornehmen. Da Internet Explorer abhängig vom jeweiligen Fall auf viele verschiedene Weisen konfiguriert werden kann, kann nur schwer eine Lösung für die erfolgreiche Verwendung von Internet Explorer mit Host Access for the Cloud und MSS angegeben werden. Folgende sind einige mögliche Konfigurationen:

- Wenn sich sowohl Host Access for the Cloud als auch MSS in der Internetzone befinden, fügen Sie den Host Access for the Cloud-Server manuell zur Zone „Lokales Intranet“ oder „Vertrauenswürdige Sites“ (Internetoptionen > Sicherheit > Lokales Intranet > Sites) hinzu. Verwenden Sie vollqualifizierte Hostnamen oder IP-Adressen.
- Wenn sich beide Server in der Zone „Internet“ befinden, ändern Sie das Standardverhalten für diese Zone, und aktivieren Sie „Cookies von Drittanbietern“ (Internetoptionen > Datenschutz > Erweitert > Automatische Cookieverarbeitung außer Kraft setzen).
- Wenn sich beide Server in der Zone „Lokales Intranet“ befinden, ändern Sie das Standardverhalten für diese Zone, und deaktivieren Sie „Kompatibilitätsansicht“ (Extras > Einstellungen der Kompatibilitätsansicht).

Probleme bei der Tastenbelegung in verschiedenen Browsern

Bestimmte Tasten auf einem numerischen Tastenfeld und einige browserspezifische Tasten können nicht zugeordnet werden. Beispielsweise können in Chrome Strg+N und Strg+W nicht zugeordnet werden.

7.18.2 Hostspezifische Probleme

Folgende Probleme beziehen sich auf spezifische Hosttypen.

Anzeigen des Euro-Zeichens

Wenn das Eurozeichen nicht ordnungsgemäß auf dem Terminalbildschirm angezeigt wird, wenden Sie sich an den Systemadministrator, um sicherzustellen, dass der Hostzeichensatz für die Sitzung korrekt eingerichtet ist. Standardmäßig verwendet Host Access for the Cloud einen Zeichensatz, der das Eurozeichen (€) nicht unterstützt. Um das Eurozeichen anzuzeigen, ändern Sie den Zeichensatz in einen Satz, der das Eurozeichen unterstützt.

Aufgetretene Probleme bei VT-Hosts

Typ	Beschreibung
Leistungsprobleme	• Eine umfangreiche Textausgabe, z. B. in der Form „Is-IR“, kann die Leistung beeinträchtigen. • Bildlaufbereiche können langsam oder verzögert angezeigt werden. • Die Cursorbewegung kann langsam oder verzögert sein. • Internet Explorer ist besonders langsam und die Leistung fällt weiter ab, wenn Zeilen und Spalten verwendet werden.
Zeichensätze	• Grafische Zeichen und einige Zeichensätze werden nicht unterstützt. • Einige nicht englische Zeichen können dazu führen, dass die Terminalanzeige einfriert.
Andere Probleme bei VT	• Das Einfügen und Löschen von Spalten (DECIC, DECDC) kann fehlschlagen. • VT400 erkennt DECSCL nicht.

Feldumrandungen in 3270-Sitzungen

Die 3270-Attribute für Feldumrandungen werden nicht vollständig unterstützt. In Host Access for the Cloud werden derzeit Unter- und Überstreichungen unterstützt, linke vertikale und rechte vertikale Linien sowie Kombinationen der vier Linientypen werden jedoch noch nicht unterstützt.

7.18.3 Probleme bei der Installation

Die Themen unter Installation und Aufrüstung enthalten einen Abschnitt zur Fehlersuche, der nützliche Informationen für die Diagnose und Behebung bestimmter Installationsprobleme bietet.

Festlegen eines temporären Verzeichnisses für das Installationsprogramm

Das Installationsprogramm benötigt Schreibzugriff auf ein temporäres Verzeichnis. Wenn das standardmäßige temporäre Verzeichnis nicht geeignet ist, kann das Installationsprogramm mit einem alternativen temporären Verzeichnis ausgeführt werden.

- Windows

  Wenn kein Schreibzugriff auf das standardmäßige temporäre Verzeichnis verfügbar ist, legen Sie die TMP- oder TEMP-Umgebungsvariablen während der Ausführung des Installationsprogramms auf ein alternatives temporäres Verzeichnis fest. Setzen Sie die Variablen nach Abschluss der Installation zurück.

- Linux/Unix

  Die Umgebungsvariable INSTALL4J_TEMP legt das Basisverzeichnis fest, das vom Installationsprogramm für die Selbstextrahierung verwendet wird. Für das Extrahieren von Dateien durch das Installationsprogramm und Starten von Java zum Ausführen anderer Aufgaben wird das temporäre Java-Verzeichnis (/tmp) verwendet.

  So führen Sie die Linux-Installationsprogramme mit einem alternativen temporären Verzeichnis aus:

  - Definieren Sie die Variable INSTALL4J_TEMP und legen Sie als Wert das gewünschte temporäre Verzeichnis fest.
  - Erstellen Sie das temporäre Verzeichnis, das Sie für das Installationsprogramm angegeben haben. Das Installationsprogramm setzt voraus, dass das Verzeichnis bereits vorhanden ist.
  - Fügen Sie beim Starten des Installationsprogramms den Kommandozeilenschalter `-J-Djava.io.tmpdir={tempdir}` hinzu. Beispiel:

```
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
```

Verkettete HACloud- und MSS-Installationen

- UnterWindows sind für eine verkettete Installation von HACloud und MSS keine weiteren Anpassungen erforderlich, wenn Sie vorübergehend die oben beschriebenen TMP- bzw. TEMP-Umgebungsvariablen festlegen.
- Unter Linux/Unix: Auf dieser Plattform können Sie keine verkettete Installation ausführen. Führen Sie die Installationen jeweils mit Administratorberechtigung separat aus. Legen Sie dabei die Variable INSTALL4J_TEMP fest und verwenden Sie den Schalter -J-Djava.io.tmpdir.

> **Hinweis**
>
> Wenn sowohl MSS als auch HACloud „unverkettet“ installiert werden, muss zuerst MSS und anschließend HACloud installiert werden.

Festlegen eines temporären Verzeichnisses für das Produkt

HACloud verwendet ein internes temporäres Verzeichnis, das in allen Fällen geeignet sein sollte. Bei Bedarf kann das Verzeichnis jedoch durch Bearbeiten der Datei `container.conf` geändert werden.

Der Speicherort kann konfiguriert werden:

1. Öffnen Sie `<Installationsordner>/sessionserver/conf/container.conf` in einem Texteditor.
2. Bearbeiten Sie die Eigenschaft wrapper.java.additional zur Angabe des neuen Speicherorts. Wenn der Pfad Leerzeichen enthält, schließen Sie ihn unter Windows in Anführungszeichen und verwenden Sie auf Linux-/Unix-Plattformen die geeignete Syntax. Beispiel: `wrapper.java.additional.9=-Djava.io.tmpdir=../tmp`
3. Bei Bedarf können Sie eine zusätzliche Eigenschaft festlegen, um das temporäre Verzeichnis beim Herunterfahren des Servers zu löschen.
4. Starten Sie den Server neu.

8. Rechtliche Hinweise