

HomeDirectory Maintenance

Ein Werkzeug zur Wartung von Benutzer-Home-Verzeichnissen bei OES.

Einführung

Werden in der OES-Umgebung Benutzer durch andere Werkzeuge als iManager o.ä. erstellt, ist es oft nicht möglich, ein Home-Directory mit anzulegen, ebenso wird – auch mit iManager – das Home-Directory beim Umbenennen des Benutzers (z.B. wegen Namensänderung durch Heirat) nicht umbenannt. Genauso bleibt beim Löschen des Benutzers ein verwaistes Verzeichnis zurück, dadurch sammeln sich im Laufe der Zeit größere Mengen potentiell unsicherer Daten auf den Platten an.

Die HomeDirectory Maintenance hilft, diese Probleme zu umgehen.

Vorgehensweise

Implementiert ist es als einzelnes Programm namens HDMaint.

HDMaint verfolgt 2 getrennte Ansätze:

- **Neuanlage**

Werden Benutzer neu angelegt, brauchen sie ein Home-Directory. Um neue Benutzer effizient zu finden, sucht HDMaint mittels LDAP in dem vorgegebenen Container (ggf. mit Sub-Containern) nach Benutzerobjekten, die seit dem letzten Lauf angelegt wurden.

Bei diesen überprüft es, ob das Attribut für das Home-Directory gesetzt ist.

Ist dieses nicht gesetzt, wird ein neues Verzeichnis (sofern nicht vorhanden) angelegt. Falls ein Verzeichnis mit dem Benutzernamen schon vorhanden ist, wird dieses genutzt. HDMaint weist dem Benutzer die eingestellten Rechte zu, setzt die Speicherplatzbeschränkung für das Verzeichnis und trägt das Verzeichnis in das Home Directory Attribut des Benutzers ein.

Ebenso wird der Benutzer als Eigentümer (Owner) des Verzeichnisses eingetragen.

Optional kann eine vorgegebene Struktur (Skeleton) in das angelegte Verzeichnis kopiert werden.

Dieser Neuanlage-Lauf ist so gestaltet, dass möglichst wenig Ressourcen und Rechenleistung belegt werden, so dass dieser oft, z.B. alle 5 Minuten per cron ausgeführt werden kann.

- **Wartung**

Beim Wartungslauf werden alle Verzeichnisse in dem Wurzelverzeichnis für die Home-Directories überprüft, mit Ausnahme derer, die mit einem Unterstrich (_) beginnen. Hier werden die verwaisten und die Verzeichnisse von umbenannten Benutzern gefunden.

Entsprechend den vorgegebenen Aktionen werden diese dann umbenannt bzw. gelöscht oder in ein anders Verzeichnis zur Überprüfung verschoben.

Wenn solche Aktionen durchgeführt wurden, kann eine entsprechende Nachricht an den Administrator generiert werden.

Voraussetzungen

HDMaint läuft auf OES24.4 und höher. Das zusätzliche Paket *libopenss/3* muss installiert sein.

Prinzipiell ist es auch auf älteren Versionen lauffähig, dazu bitte anfragen. Eventuell ist für OES ab 25.4 (SLES15 SP7 basiert) eine neu compilierte Version nötig. Diese wird zeitnah zum Erscheinen der entsprechenden Version zur Verfügung gestellt.

HDMaint ist cluster-aware. Beim Start wird überprüft, ob das zu überprüfende Volume gemountet ist. Falls nicht, beendet sich HDMaint stillschweigend. Dadurch kann es auf allen Cluster-Nodes, auf denen das Home-Directory-Volume laufen könnte, installiert werden.

Da HDMaint auf Schnittstellen zugreift, die nur dem Benutzer root zugänglich sind, muss es von dem Benutzer root ausgeführt werden.

Installation

Zur Installation kopieren Sie die ausführbaren Dateien HDMaint in ein beliebiges Verzeichnis des Servers, z.B. /opt/HDMaint und machen sie ausführbar (chmod +x HDMaint)

Haben Sie ein Archiv erhalten, entpacken Sie es bitte in ein Verzeichnis wie oben, es sollte bereits eine als ausführbar gekennzeichnete Datei HDMaint enthalten.

Konfiguration

Die Konfiguration erfolgt über eine .ini Datei. Standardmäßig hat diese den Namen HDMaint.ini. Es können über den Parameter -f oder --inifile auch andere Dateinamen z.B. für mehrere Konfigurationen angegeben werden.

Pfade in der Konfiguration (HDBase, MoveTarget, Skeleton) werden ohne führenden Delimiter und mit einem Schrägstrich (/) angegeben.

Hier ein Beispiel:

```
[LDAP]
LDAPHost=172.16.129.1
LDAPUser=cn=admin,o=bond
LDAPPass=XXXXXXX
LDAPCont=O=Test
LDAPScope=o

[Path]
VolObj=cn=James12_USER,ou=Server,O=bond
VolName=USER
HDBase=Test
OrphanAction=DELETE
MoveTarget=Test/_Delete.me
Skeleton=Test/_Skele.ton
SkelCopy=TRUE

[Dir]
FolderRights=rwcmf
DirQuota=10GB
AdjustQuota=TRUE

[Log]
LogLevel=1
LogDir=log
LogMax=10M

[RUN]
TickCount=10
Ticker=1
LastRun=20251118211737Z
```

Die Parameter in der ini-Datei im Einzelnen:

Sektion	Name	Beschreibung
---------	------	--------------

LDAP	LDAPHost	IP-Adresse oder DNS Name des LDAP-Hosts, am einfachsten der Server selbst.
LDAP	LDAPUser	Benutzername im LDAP-Format, sollte Leserechte und das Schreibrecht auf das Home Directory Attribut haben
LDAP	LDAPPass	Passwort des LDAP-Users. Es wird beim ersten Start von HDMaint verschlüsselt
LDAP	LDAPCont	LDAP-Context: Start-Kontext für die Suche nach neu angelegten Benutzern
LDAP	LDAPScope	Suchbereich: o bedeutet, nur der angegebene Kontext, s auch die untergeordneten Kontexte
Path	VolObj	Name des Volume-Objektes im LDAP-Format
Path	VolName	Volume Name – Vorsicht Groß/Kleinschreibung wird unterschieden
Path	HDBase	Falls die Benutzerverzeichnisse nicht direkt im Hauptverzeichnis des Volume sind, kann hier ein Unterverzeichnis angegeben werden. Auch hier: Vorsicht Groß/Kleinschreibung wird unterschieden
Path	OrphanAction	Legt fest, wie mit „verwaisten“ Verzeichnissen zu verfahren ist. MOVE bedeutet Verschieben in das MoveTarget Verzeichnis, DELETE bedeutet löschen. Ist diese Option leer oder ungültig, bleiben die Verzeichnisse bestehen.
Path	MoveTarget	Das Verzeichnis, in das die verwaisten Verzeichnisse verschoben werden sollen, relativ zum Volume (Es kann nur innerhalb des Volumes verschoben werden), ohne führenden Schrägstrich. Der Name sollte mit einem Unterstrich (_) anfangen, da Verzeichnisse mit Unterstrich beim Check ignoriert werden.
Path	Skeleton	Falls SkelCopy TRUE ist, werden die in diesem Verzeichnis liegenden Unterverzeichnisse und Dateien in das neue HomeDirectory kopiert. Der Name sollte ebenfalls mit einem Unterstrich beginnen, falls er sich innerhalb des HDBase-Verzeichnisses befindet (oder HDBase leer ist)
Path	SkelCopy	Falls True -> siehe oben
Dir	FolderRights	Die zu vergebenden Rechte des Benutzers auf das Verzeichnis, in Form einer Liste aus Kleinbuchstaben: r = read w=write c=create e=erase m=modify (gemeint ist hier umbenennen etc.) f=file scan a= access control s=supervisor
Dir	DirQuota	Die Speicherplatzbeschränkung für das Verzeichnis in KB, MB oder GB. Sollte ein Vielfaches von 4KB sein.
Dir	AdjustQuota	Gibt an, ob ein existierendes Quota, das kleiner ist als DirQuota, angepasst werden soll. TRUE => Ja, FALSE = Nein
Log	LogLevel	Details der Ausgabe in das Logfile: 0: Keine Ausgabe 1: (Standard) Ausgabe bei Änderungen, d.h. neue Benutzer, Umbenennungen oder Löschungen 2: zusätzlich bei jedem Lauf eine Zeile, welcher Lauf ausgeführt wurde (check oder make) 3: komplette Ausgabe wie bei Interactive
Log	LogDir	Verzeichnis für das logfile. Hat der Wert keinen führenden „/“ dann wird das Verzeichnis relativ zum Standort der Programmdatei ausgewertet,

		ansonsten absoluter Pfad. Standard: log Die Logdatei heißt HDMaint.log
Log	LogMax	Maximale Größe für das Logfile. Wird diese Größe überschritten, wird das alte logfile umbenannt, indem das Datum angehängt wird. Dann wird ein neues begonnen.
RUN	TickCount	Anzahl der Make-Läufe, nach denen ein Check-Lauf erfolgt.
RUN	Ticker	Aktueller Zähler der Make-Läufe, erreicht dieser den Wert TickCount, wird anstelle des Make-Laufs ein Check-Lauf ausgeführt. Anschließend wird der Wert wieder auf 1 zurückgesetzt.
RUN	LastRun	Der LDAP Zeitstempel (JJJJMMTThhmmssZ) der letzten Ausführung (minus 1 Minute). Wird bei jeder Ausführung von Check oder Make aktualisiert.

Wird HDMaint mit dem Parameter -g aufgerufen, erstellt es eine leere .ini-Datei, falls diese nicht schon vorhanden ist.

Kommandozeilen-Optionen

HDMaint ist primär zur Ausführung per cron gedacht. Mehr dazu im Abschnitt Automatisierung.

Interactive (-i)

Da HDMaint normalerweise per cron ausgeführt wird, erfolgt keine Ausgabe. Diese Option schaltet die Ausgabe von Aktionen und Fehlern ein.

Sie sollten nach Erstellen oder Ändern der Konfiguration mindestens einmal HDMaint über die Kommandozeile mit dieser Option aufrufen, um zu überprüfen, ob es wunschgemäß ausgeführt wird.

DryRun (-d)

Führt einen Trockenlauf durch. Gilt für die Optionen Make (-m) und Check (-c). Anstelle der echten Veränderungen werden lediglich Meldungen ausgegeben. Beinhaltet die Option Interactive.

Version (-v)

Diese Option gibt die Version, den aktuellen Baumnamen, Context, die Anzahl der Benutzerobjekte und die Lizenzierungsinformationen aus.

ListDir (-l)

Diese Option schließt Interactive mit ein. Sie gibt zwei Listen aus:

Die Benutzer (aus LDAP) mit deren HomeDirectory-Attribut und

Die Verzeichnisse aus dem Basisverzeichnis mit Quotas, Eigentümern und Rechtezuweisungen

Make (-m)

Dieses ist die Option, die per cron ausgeführt werden sollte. Sie führt abhängig vom Stand des Tickers einen Make- oder einen Check-Lauf (s.unten) aus.

Die Make-Operation ist bewusst sparsam ausgelegt, um Ressourcen zu sparen, so dass sie ohne Probleme oft ausgeführt werden kann (z.B. alle 5 Minuten)

Make fragt per LDAP nach neuen Benutzerobjekten seit der letzten Ausführung (ini-Parameter LastRun). Sind neue Objekte erstellt worden, erzeugt es die passenden Home-Directories und kopiert optional den Inhalt des Skeleton-Verzeichnisses hinein.

Check (-c)

Der Check-Lauf wird automatisch alle TickCount Male anstelle des Make-Laufs ausgeführt. Mit dieser Option kann er aber auch (zur Kontrolle) direkt ausgeführt werden. Der Check führt 2 Aktionen aus:

Für alle LDAP Benutzer (entsprechend der Vorgabe): Überprüfen, ob ein HomeDirectory zugewiesen wurde und ob es den gleichen Namen wie der Benutzer hat. Falls es hier Abweichungen gibt, werden diese korrigiert. Damit werden Umbenennungen erkannt und auf das Verzeichnis angewandt.

Für alle Verzeichnisse (im Basisverzeichnis): Überprüfen, ob ein Benutzer zugeordnet ist. Falls ja werden die Rechte und die Quota-Zuweisung überprüft. Falls weniger Speicherplatz erlaubt ist als die Vorgabe, oder falls keine Einschränkung besteht, wird die Platzbeschränkung laut Vorgabe zugewiesen. Falls keine Rechte existieren, werden die Rechte laut Vorgabe eingestellt. Weiterhin wird die Eigentümer-Zuweisung überprüft und ggf. korrigiert. Falls kein zugeordneter Benutzer existiert, wird das Verzeichnis entweder in das Zielverzeichnis für verwaiste Verzeichnisse verschoben, gelöscht oder ignoriert.

Prune (-p)

Löscht das als Parameter angegebene Verzeichnis (absoluter Pfad) inklusive aller Unterverzeichnisse und Dateien. Sollten Attribute wie Deletelnhibit gesetzt sein, werden diese vorher zurückgesetzt.

OrphanPrune (-o)

Löscht den Inhalt des als Zielverzeichnis für verwaiste HomeDirectories angegebenen Verzeichnisses, ebenfalls mittels Zurücksetzens der Attribute, die ein Löschen verhindern könnten.

GenIni (-g)

Erzeugt eine Vorlage für die .ini-Datei im aktuellen Verzeichnis.

Automatisierung

Zum Aktivieren der Funktion wird der Aufruf von HDMaint in die crontab von root eingetragen:

```
# crontab -e
```

Im Editor (standardmäßig vi bzw. vim) mit <Umschalt> A eine neue Zeile anfangen und folgendes eintragen:

```
*/5 * * * * /opt/HDMaint/HDMaint -m
```

Wenn HDMaint in einem anderen Ordner installiert ist, den entsprechenden Ordner angeben.

Dann den Editor mit <Esc> : wq verlassen.

Lizenz

HDMaint enthält bereits eine freie Lizenz für einen beliebigen Baumnamen und 50 Benutzerobjekte. Falls Ihr Benutzercontainer mehr als 50 Benutzer enthält, müssen Sie eine Lizenz kaufen. Diese Lizenz bezieht sich auf den Baumnamen und ggf. die Anzahl der Benutzer. Mit der Option -v können Sie beides herausfinden.

Haben Sie eine Lizenz erworben, erhalten Sie eine Lizenzdatei, die HDMaint.lic heißen sollte. Diese Datei muss sich im gleichen Verzeichnis wie HDMaint befinden. Es kann sein, dass Sie aus organisatorischen Gründen eine Lizenzdatei erhalten, die nicht HDMaint.lic heißt. In diesem Falle benennen Sie sie einfach um.

Nach der Installation der Lizenzdatei sollten Sie ebenfalls mit der Option -v prüfen, ob die Lizenz erkannt wird.

Versionen

1.0 (20.11.2025)

Erste Veröffentlichung

1.1 (23.11.2025)

Schnittstelle zu NIT (Network Identity Translator) hinzugefügt, da einige GUID aus LDAP nicht den GUIDs von NSS entsprechen.

1.2 (26.11.2025)

Logging hinzugefügt