Oracle® DIVAdirector

Sicherheitshandbuch

Release 5.3

E71130-01

Dezember 2015

ORACLE®

Oracle® DIVAdirector
Sicherheitshandbuch

E71130-01

Inhalt

Vorwort

Das Oracle DIVAdirector - Sicherheitshandbuch enthält Informationen zum Produkt DIVAdirector und Erläuterungen allgemeiner Grundsätze sicherer Anwendungen.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung von Sicherheitsfunktionen und der sicheren Installation und Konfiguration von DIVAdirector beteiligt sind.

Barrierefreie Dokumentation

Informationen über Eingabehilfen für die Dokumentation finden Sie auf der Oracle Accessibility Program-Webseite unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Zugang zum Oracle-Support
Oracle-Kunden mit einem gültigen Oracle-Supportvertrag haben Zugriff auf elektronischem Support über My Oracle Support. Weitere Informationen erhalten Sie unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oder unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs, falls Sie eine Hörbehinderung haben.

1

Kapitel 1. Überblick

Dieses Kapitel enthält einen Überblick zum Produkt DIVAdirector und Erläuterungen allgemeiner Grundsätze sicherer Anwendungen.

1.1. Produktüberblick

Oracle DIVAdirector dient zur Interaktion mit vorhandenen Oracle DIVArchive-Systemen. Die Benutzeroberfläche (User Interface, UI) wird grafisch über einen Webbrowser bereitgestellt. DIVAdirector besteht aus den folgenden Hauptkomponenten:

1.1.1. DIVAdirector Server

DIVAdirector Server stellt Schnittstellen zu DIVArchive über die C++ API für alle Vorgänge bereit, die von DIVAdirector Web angefordert werden. Darüber hinaus synchronisiert das Tool die ermittelten Objektinformationen, die in DIVArchive gespeichert sind, mit seiner eigenen Datenbank. Es überwacht konfigurierte Drop-Ordner für Proxys, Metadaten und Vorgänge und speichert eine Historie aller Drop-Ordner und UI-Vorgänge.

1.1.2. DIVAdirector Web

Das Webmodul von DIVAdirector stellt eine webbasierte UI-Schnittstelle bereit, die es Benutzern ermöglicht, nach ermittelten Objekten in DIVArchive zu suchen, Benutzerzugriffsrechte zu verwalten, Metadaten für Assets hinzuzufügen, als Stellvertreter für Objekte zu fungieren und an Elementen, die Arbeits-Bins oder Aufnahmelisten hinzugefügt wurden, Vorgänge wie Wiederherstellen (ganz oder teilweise) oder Löschen auszuführen. Benutzer können damit außerdem Dateien lokal durchsuchen und Inhalte im DIVArchive-System archivieren.

1.1.3. DIVAdirector Database

DIVAdirector verwendet PostgreSQL für die Speicherung aller DIVArchive-Assetinformationen, Metadaten, Proxyinformationen, Benutzerinformationen, der Vorgangshistorie und Konfigurationseinstellungen.

1.1.4. DIVAdirector Transcoder Service

DIVAdirector Transcoder Service ist ein separater Service, der von DIVAdirector aufgerufen wird, um Clips mit hoher Auflösung in Proxys mit niedriger Auflösung umzuwandeln, die dann in der DIVAdirector Web-UI dargestellt werden.

1.1.5. DIVAdirector Task Manager Service

DIVAdirector Task Manager Service ist eine Windows-basierte Serviceanwendung, die im Standarddialogfeld "Services Control Manager" angezeigt wird. Diese Anwendung ist dafür zuständig, Aufgaben, die möglicherweise eine lange Ausführungszeit besitzen, in einem Hintergrundprozess auszuführen.

1.1.6. DIVAdirector API Service

Dieser Service zeigt Endpunkte für allgemeine DIVAdirector-Funktionen an. Anfänglich wird dieser Service nur eine geringe Teilmenge der Logik von DIVAdirector umfassen. Durch die allmähliche Umlenkung der Funktionen von DIVAdirector Web weg wird die Anzahl der durch diesen Service angezeigten Endpunkte weiter zunehmen.

1.2. Allgemeine Sicherheitsgrundsätze

In den folgenden Abschnitten werden die Grundsätze beschrieben, die für eine sichere Verwendung von Anwendungen unerlässlich sind.

1.2.1. Software muss immer auf dem neuesten Stand sein

Bringen Sie die DIVAdirector-Version, die Sie ausführen, immer auf den neuesten Stand. Sie können die aktuellen Versionen der Software unter Oracle Software Delivery Cloud herunterladen:

https://edelivery.oracle.com/

1.2.2. Netzwerkzugriff muss auf kritische Services begrenzt sein

DIVAdirector verwendet folgende TCP/IP-Ports:

- tcp/7680 für Befehle aus der Benutzeroberfläche
- tcp/8080 für den HTTP-Server

Für DIVAdirector-Releases höher als 5.3.0 werden drei zusätzliche Ports benötigt:

- tcp/9763 - DIVArchiveWS Service-Integration.
- tcp/9876 - DIVAtranscode Service-Integration.
- tcp/6543 - DIVAdirector API Service-Integration.

Hinweis:

Die oben aufgeführten Portnummern sind auf dem neuesten Stand, sind jedoch vermutlich Änderungen unterworfen.

1.2.3. Die Ausführung muss als ADMIN-Benutzer unter Verwendung des Prinzips der geringsten Berechtigungsstufe erfolgen, sofern möglich

DIVAdirector stellt ein Standard-Superadministratorkonto bereit, dessen Passwort nach der erstmaligen Anmeldung geändert werden muss. Dieser Benutzer kann dann weitere Benutzer mit unterschiedlichen Gruppenberechtigungen für den Zugriff und für Vorgänge erstellen.

Wenn das Standardpasswort nicht geändert wird, wird das System anfällig für böswillige Angriffe. Das Standardpasswort für das Superadministratorkonto muss umgehend nach der Installation und Konfiguration geändert werden, und danach (mindestens) alle 180 Tage. Hinterlegen Sie die Passwörter nach der Änderung offline an einem sicheren Ort, wo sie Oracle Support bei Bedarf zur Verfügung gestellt werden können.

1.2.4. Überwachen der Systemaktivität

Sie können die Systemaktivität überwachen, um die Funktionsqualität von DIVAdirector zu bestimmen. Protokolle werden unter C:/Program Files (x86)/DIVAdirector 5/cmg-server und C:/Program Files (x86)/DIVAdirector 5/www/logs gespeichert.

1.2.5. Sicherheitsinformationen müssen immer auf dem neuesten Stand sein

Sie können Sicherheitsinformationen aus mehreren Quellen erhalten. Sicherheitsinformationen und Warnungen für zahlreiche Produkte finden Sie unter:

`http://www.us-cert.gov`

Sie bleiben hinsichtlich der Sicherheit vor allem dann auf dem neuesten Stand, wenn Sie die neueste Version der DIVAdirector-Software ausführen.

2

Kapitel 2. Sichere Installation

In diesem Kapitel wird der Planungsprozess für eine sichere Installation beschrieben. Außerdem werden mehrere empfohlene Deployment-Topologien für die Systeme beschrieben.

2.1. Ihre Umgebung

Zum besseren Verständnis der Sicherheitsanforderungen müssen die folgenden Fragen gestellt werden:

2.1.1. Welche Ressourcen müssen geschützt werden?

In der Produktionsumgebung können zahlreiche Ressourcen gesichert werden. Berücksichtigen Sie bei der Bestimmung der Sicherheitsstufe den zu sichernden Ressourcentyp. Schützen Sie bei der Verwendung von DIVAdirector die folgenden Ressourcen:

2.1.1.1. Primärer Datenträger für Daten

Hierbei handelt es sich um Proxyordner, die Clips mit niedriger Auflösung enthalten. Diese befinden sich hauptsächlich auf lokalen oder Remote-Datenträgern, die mit dem DIVAdirector-System verbunden sind. Ein unabhängiger Zugriff auf diese Datenträger (nicht über DIVAdirector) stellt ein Sicherheitsrisiko dar. Diese Form des externen Zugriffs kann von einem Rogue-System stammen, das von diesen Datenträgern liest oder darauf schreibt, oder von einem internen System, das unbeabsichtigt Zugriff auf diese Datenträgergeräte gewährt.

2.1.1.2. Datenbankdatenträger und Backupdatenträger

Hierbei handelt es sich um Datenbank- und Backupdatenträgerressourcen, mit denen DIVAdirector erstellt wird. Dies sind üblicherweise lokale oder Remote-Datenträger, die mit den DIVAdirector-Systemen verbunden sind. Ein unabhängiger Zugriff auf diese Datenträger (nicht über DIVAdirector) stellt ein Sicherheitsrisiko dar. Diese Form des externen Zugriffs kann von einem Rogue-System stammen, das von diesen Datenträgern liest oder darauf schreibt, oder von einem internen System, das unbeabsichtigt Zugriff auf diese Datenträgergeräte gewährt.

2.1.1.3. Konfigurationsdateien und Einstellungen

Die Konfigurationseinstellungen des DIVAdirector-Systems müssen vor Betriebssystembenutzern ohne Administratorrechte geschützt werden. Im Allgemeinen werden diese Einstellungen automatisch durch Betriebssystembenutzer mit Administratorrechten geschützt. Beachten Sie, dass ein Sicherheitsrisiko entsteht, wenn andere BS-Benutzer als der Administrator in Konfigurationsdateien schreiben können. Vertrauliche Dateien umfassen alle Anwendungskonfigurationsdateien, die im Installationsverzeichnis enthalten sind, darunter:

- www/Web.config
- Api/Oracle.DIVAdirector.Api.exe.config
- TaskManager/Oracle.DIVAdirector.TaskManager.exe.config
- cmgserver/cmgserver.ini

2.1.2. Vor wem müssen die Ressourcen geschützt werden?

Im Allgemeinen müssen die auf einem konfigurierten System im vorherigen Abschnitt beschriebenen Ressourcen vor sämtlichen Zugriffen geschützt werden. Dazu gehören auch Zugriffe eines externen Rogue-Systems über WAN oder FC-Fabric. Administratorenzugriffe sind davon nicht betroffen.

2.1.3. Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?

Die Ursachen für das Versagen des Schutzes strategischer Ressourcen können von unberechtigten Zugriffen (Datenzugriffe, die den normalen DIVAdirector-Vorgängen nicht entsprechen) bis hin zu Datenbeschädigungen (Schreiben auf Datenträger oder Band außerhalb der normalen Berechtigungen) reichen.

3

Kapitel 3. Sicherheitsfunktionen

Zur Vermeidung möglicher Sicherheitsrisiken müssen sich Benutzer von DIVAdirector mit der Authentifizierung und Autorisierung des Systems befassen.

Diese Sicherheitsrisiken können durch ordnungsgemäße Konfiguration und Befolgen der Checkliste nach Abschluss der Installation in Anhang A, *Checkliste für sicheres Deployment* minimiert werden.

3.1. Das Sicherheitsmodell

Die folgenden kritischen Sicherheitsfunktionen bieten Schutz vor Sicherheitslücken:

- Authentifizierung – Dadurch wird sichergestellt, dass nur berechtigten Personen Zugriff auf System und Daten gewährt wird.
- Autorisierung – Der Zugriff auf Systemberechtigungen und -daten wird kontrolliert. Diese Funktion baut auf der Authentifizierung auf, um zu gewährleisten, dass Benutzer nur den für sie vorgesehenen Zugriff erhalten.

Anhang A

Anhang A. Checkliste für sicheres Deployment

1. Legen Sie starke Passwörter für das Administrator- und sonstige BS-Konten fest, denen DIVArchive- oder DIVAdirector-Administrator- oder Servicerollen zugewiesen sind.
2. Verwenden Sie kein lokales BS-Administratorkonto, sondern weisen Sie Rollen nach Bedarf anderen Benutzerkonten zu.
3. Legen Sie ein starkes Passwort für den DIVAdirector-Admin-Benutzer fest. Ändern Sie das bei der Installation zugewiesene Standardpasswort umgehend in ein starkes Passwort. Sie können dies auf dem DIVAdirector-Einstellungsbildschirm unter **Admin**, **Personal** vornehmen.
4. Installieren Sie eine Firewall in dem System, und übernehmen Sie die DIVAdirector-Standardportregeln.
5. Installieren Sie in regelmäßigen Abständen BS- und DIVAdirector-Updates, da diese Sicherheitspatches beinhalten.
6. Installieren Sie ein Antivirenprogramm, und schließen Sie die DIVAdirector-Prozesse und -Speicherung aus Performancegründen aus.