

Oracle® DIVArchive

Sicherheitshandbuch

Release 7.3

E70869-01

Dezember 2015

Copyright © 2015, Oracle und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, dann gilt Folgendes:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. UNIX ist eine eingetragene Marke von The Open Group.

Diese Software oder Hardware und die Dokumentation können Zugriffsmöglichkeiten auf oder Informationen über Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Inhalt

Vorwort	5
Zielgruppe	5
Barrierefreie Dokumentation	5
1. Überblick	7
1.1. Produktüberblick	7
1.1.1. DIVArchive Manager	7
1.1.2. DIVArchive Actor	7
1.1.3. DIVArchive Robot Manager	7
1.1.4. DIVArchive Backup Service	8
1.1.5. Oracle Avid-Konnektivität	8
1.1.6. DIVArchive Drop Folder Monitor	8
1.1.7. DIVArchive SNMP	8
1.1.8. DIVArchive SPM	9
1.1.9. DIVArchive Migrate Service	9
1.1.10. DIVArchive VACP	9
1.1.11. Grafische DIVArchive-Kontrollbenutzeroberfläche	9
1.1.12. DIVArchive-Konfigurationsdienstprogramm	9
1.1.13. DIVArchive Access Gateway	9
1.1.14. DIVArchive Lynx Local Delete	10
1.2. Allgemeine Sicherheitsgrundsätze	10
1.2.1. Software muss immer auf dem neuesten Stand sein	10
1.2.2. Netzwerkzugriff auf kritische Services begrenzen	10
1.2.3. Ausführung als DIVA-Benutzer und Verwendung des Prinzips der geringsten Berechtigungen wenn möglich	10
1.2.4. Systemaktivität überwachen	11
1.2.5. Sicherheitsinformationen immer auf dem neuesten Stand halten	11
2. Sichere Installation	13
2.1. Umgebung analysieren	13
2.1.1. Welche Ressourcen müssen geschützt werden?	13
2.1.1.1. Primärer Datenträger	13
2.1.1.2. Datenbankdatenträger, Metadatendatenträger und Backupdatenträger	13
2.1.1.3. DIVArchive-Bänder	14

- 2.1.1.4. Exportieren von Bandmetadaten 14
- 2.1.1.5. Konfigurationsdateien und Einstellungen 14
- 2.1.2. Vor wem werden die Ressourcen geschützt? 14
- 2.1.3. Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt? 14
- 2.2. Empfohlene Deployment-Topologien 14
 - 2.2.1. Separates Metadatenetzwerk 14
 - 2.2.2. FC-Zoning 15
 - 2.2.3. Absichern des Zugriffs auf SAN-Datenträgerkonfiguration 15
 - 2.2.4. Installieren des DIVArchive-Packages 15
 - 2.2.5. DIVArchive-Bandsicherheit 15
 - 2.2.6. Backups 15
- 2.3. Konfiguration nach Abschluss der Installation 15
- 3. Sicherheitsfunktionen 17**
 - 3.1. Sicherheitsmodell 17
 - 3.2. Authentifizierung 17
 - 3.3. Zugriffskontrolle 17
- A. Prüfliste für sicheres Deployment 19**

Vorwort

Oracle DIVArchive - Sicherheitshandbuch umfasst Informationen zu dem DIVArchive-Produkt und erläutert die Grundlagen der Anwendungssicherheit.

Zielgruppe

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

Kapitel 1. Überblick

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

1.1. Produktüberblick

Oracle DIVArchive ist ein verteiltes System zur Verwaltung der Inhaltsspeicherung. DIVArchive besteht aus den folgenden Hauptkomponenten:

1.1.1. DIVArchive Manager

DIVArchive Manager ist die Hauptkomponente in einem DIVArchive-System. Alle Archivierungsvorgänge werden vom DIVArchive Manager kontrolliert und verarbeitet. Vorganganforderungen werden von Initiatoranwendungen über die DIVArchive-Client-API gesendet. Als kostenpflichtige Option unterstützt DIVArchive auch Haupt- und Backup-DIVArchive Manager. Weitere Informationen zu DIVArchive finden Sie in der DIVArchive Software Release 7.3 Customer Documentation Library unter:

<https://docs.oracle.com/en/storage/#csm>

1.1.2. DIVArchive Actor

DIVArchive Actor ist für die Datenverschiebung zwischen Geräten im Production-System zuständig. Diese Komponente unterstützt den Datentransfer zwischen vielen verschiedenen Gerätetypen und verarbeitet Transcodierungsvorgänge mit Telestream-Transcodierungssoftware (optional).

Alle Actor-Vorgänge werden von DIVArchive Manager gestartet und koordiniert. Ein einzelner DIVArchive Manager kann ein oder mehrere Actor konfigurieren und kontrollieren.

1.1.3. DIVArchive Robot Manager

Auch wenn DIVArchive nur zur Verwaltung des Datenspeichers verwendet werden kann, kann die Speicherkapazität doch erweitert werden, indem eine oder mehrere Bandbibliotheken hinzugefügt werden. In diesen Fällen stellt das DIVArchive Robot Manager-Modul eine Zwischensoftwareschicht bereit, damit DIVArchive Manager mit vielen verschiedenen Typen von Bandbibliotheken kommunizieren kann. Sie ist über TCP/IP mit DIVArchive Manager verbunden. DIVArchive Robot Manager stellt eine Verbindung zu der Bibliothek entweder mit einer direkten Schnittstelle zu der Bibliothek

selbst (über systemeigenes SCSI oder SCSI über Fiber Channel) oder über eine Ethernet-Zwischenverbindung zu der Bibliothekskontrollsoftware des Herstellers selbst her.

1.1.4. DIVArchive Backup Service

Um Verlässlichkeit und Überwachung sowohl der Backups von Oracle Database als auch der Backups der Metadatendatenbank zu gewährleisten, wurde der DIVArchive Backup Service eingeführt.

Die DIVArchive Backup Service-Komponente wird als integraler Bestandteil der Standard-DIVArchive-Systeminstallation installiert. Die Komponente wird im Allgemeinen auf demselben Server wie DIVArchive Manager und Oracle Database installiert. DIVArchive Backup Service lässt die Konfiguration geplanter Backups über seine Konfigurationsdatei zu. DIVArchive Backup Service verwaltet und überwacht den gesamten Backupprozess.

DIVArchive Backup Service umfasst jetzt die Möglichkeit, E-Mails zu Problemen zu versenden, die beim Backup von Datenbank- und Metadatendatenbankdateien entstehen. Um diese Funktion nutzen zu können, muss DIVArchive so konfiguriert sein, dass Verbindung zu einem SMTP-Mailprovider besteht. Die E-Mail-Benachrichtigungen werden über das DIVArchive-Konfigurationsdienstprogramm unter der Registerkarte "Manager Setting" konfiguriert.

Informationen zur Installation und Konfiguration des DIVArchive Backup Service finden Sie in der DIVArchive Software Release 7.3 Customer Documentation Library unter:

<https://docs.oracle.com/en/storage/#csm>

1.1.5. Oracle Avid-Konnektivität

Die Avid-Konnektivität mit DIVArchive soll die Übertragung von Archivierungsdaten zu und von DIVArchive in spezifischen Videoformaten sowie die Archivierung und den Abruf einzelner Clips oder Clipsequenzen ermöglichen. Die AMC- und TMC-bezogenen Komponenten werden zusammen mit der DIVArchive-Hauptinstallation installiert. Bei bestimmten Plug-ins für AMC und TMC ist eine zusätzliche Installation erforderlich.

1.1.6. DIVArchive Drop Folder Monitor

DIVArchive Drop Folder Monitor (DFM) ermöglicht die automatische Überwachung neu erstellter Dateien in maximal 20 lokalen Ordnern und/oder FTP-Ordnern. Eine oder mehrere Dateien (in FTP-Ordnern) pro DIVArchive-Objekt werden unterstützt. Wenn eine neue Datei (oder ein neuer FTP-Ordner) identifiziert wird, gibt DMF automatisch eine Anforderung an DIVArchive zur Archivierung der neuen Datei oder der neuen Ordner aus. Nachdem diese Dateien erfolgreich archiviert wurden, werden sie automatisch aus der Quelle gelöscht.

1.1.7. DIVArchive SNMP

DIVArchive SNMP (Simple Network Management Protocol) Agent und Management Information Base (MIB) unterstützen Überwachung von Status und Aktivität von DIVArchive

und dessen Subsystemen über eine Überwachungsanwendung eines anderen Herstellers über das SNMP-Protokoll.

1.1.8. DIVArchive SPM

DIVArchive Storage Plan Manager (SPM) stellt die automatische Migration und Verwaltung des Lebenszyklus von Material innerhalb des Archivs basierend auf den Regeln und Richtlinien bereit, die in der SPM-Konfiguration definiert sind.

Mit der SPM-Komponente wird auch das Löschen von Material aus den von SPM verwalteten Arrays ausgelöst (basierend auf Grenzwerten für die Datenträgerkapazität).

1.1.9. DIVArchive Migrate Service

DIVArchive umfasst einen eingebetteten Migrationsservice. Dies ist ein neuer und separater interner Service (in DIVArchive), mit dem Benutzer Jobs zur Migration von Inhalten zwischen verschiedenen Medien innerhalb eines DIVArchive-Systems planen und ausführen können. Sie können die grafische Kontrollbenutzeroberfläche oder den Befehlszeilenclient verwenden.

1.1.10. DIVArchive VACP

VACP (Video Archive Command Protocol) ist ein von Harris Automation entwickeltes Protokoll zur Verbindung mit einem Archivierungssystem. DIVArchive verfügt über eine eigene API zur Kommunikation mit DIVArchive Manager, die nicht mit VACP kompatibel ist.

1.1.11. Grafische DIVArchive-Kontrollbenutzeroberfläche

Mit der grafischen DIVArchive-Kontrollbenutzeroberfläche werden Vorgänge in DIVArchive überwacht, kontrolliert und beaufsichtigt. Verschiedene grafische DIVArchive-Benutzeroberflächen können gleichzeitig ausgeführt und mit demselben DIVArchive-System verbunden werden.

1.1.12. DIVArchive-Konfigurationsdienstprogramm

Mit dem DIVArchive-Konfigurationsdienstprogramm wird ein DIVArchive-System konfiguriert. Auch wenn es in erster Linie zur Konfiguration von DIVArchive verwendet wird, werden auch einige Betriebsfunktionen mit dem Konfigurationsdienstprogramm ausgeführt.

1.1.13. DIVArchive Access Gateway

Mit Access Gateway können mehrere unabhängige DIVArchive-Systeme von einem einzelnen Computer aus betrieben werden und miteinander kommunizieren. Dies ist die globale Lösung für die Inhaltsverteilung. Die automatisierte Dateireplikation auf gespiegelte Sites ist eine saubere und einfache Methode für lokale Verteilung, Backup und Disaster

Recovery mit Sicherheit, Bandbreitenkontrolle und Prüfsummenverifizierung. Netzwerke werden überwacht und DIVAnet stellt die abschließende Zustellung des Inhalts sicher.

1.1.14. DIVArchive Lynx Local Delete

LYNXLocalDelete ist ein Service, der Funktionen der Objektreplikation zwischen einem lokalen DIVArchive- System (z.B. LYNXlocal) und einem (oder mehreren) Remote-DIVArchive-Systemen (z.B. LYNXdr) überwacht. Nachdem das Objekt erfolgreich auf dem Remote-DIVArchive-System repliziert wurde, wird es zur Löschung aus dem lokalen DIVArchive-System gekennzeichnet.

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

DIVArchive-Version, die Sie ausführen, muss immer auf dem neuesten Stand sein. Sie können die aktuellen Versionen der Software unter Oracle Software Delivery Cloud herunterladen:

<https://edelivery.oracle.com/>

1.2.2. Netzwerkzugriff auf kritische Services begrenzen

DIVArchive verwendet folgende TCP/IP-Ports:

- tcp/8500 wird von DIVArchive Robot Manager verwendet
- tcp/9000 wird von DIVArchive Manager verwendet
- tcp/9300 wird von DIVArchive Backup Service verwendet
- tcp/9500 wird von DIVArchive Access Gateway verwendet
- tcp/9900 wird von DIVArchive Actor verwendet
- tcp/9191 wird von DIVArchive Migrate Service verwendet

1.2.3. Ausführung als DIVA-Benutzer und Verwendung des Prinzips der geringsten Berechtigungen wenn möglich

Alle DIVArchive-Services werden als DIVA-Benutzer ausgeführt. Die grafische DIVArchive-Kontrollbenutzeroberfläche stellt drei feste Benutzerprofile bereit (Administrator, Operator und Benutzer). Für den Zugriff auf die Administrator- und Operatorkonten ist ein Passwort erforderlich. In dem DIVArchive-System sind bereits Standardpasswörter installiert, die jederzeit mit dem DIVArchive-Konfigurationsdienstprogramm geändert werden können. Wenn die Standardpasswörter nicht geändert werden, ist das DIVArchive-System für böswillige Aktivitäten anfällig. **Standardpasswörter müssen sofort nach der Installation und Konfiguration der Administrator- und Operatorkonten und danach (mindestens)**

alle 180 Tage geändert werden. Nachdem die Änderung vorgenommen wurde, müssen Sie die Passwörter an einem sicheren Ort, offline, aufbewahren, damit sie gegebenenfalls Oracle Support zur Verfügung gestellt werden können.

1.2.4. Systemaktivität überwachen

Überwachen Sie die Systemaktivität, um festzustellen, wie gut DIVArchive arbeitet und ob ungewöhnliche Aktivitäten protokolliert werden. Prüfen Sie die Logdateien im Installationsverzeichnis unter /Program/log/.

1.2.5. Sicherheitsinformationen immer auf dem neuesten Stand halten

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 DIVArchive-Software ausführen.

Kapitel 2. Sichere Installation

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

2.1. Umgebung analysieren

Damit Sie die Sicherheitsanforderungen besser verstehen, müssen die folgenden Fragen gestellt werden:

2.1.1. Welche Ressourcen müssen geschützt werden?

In der Production-Umgebung können zahlreiche Ressourcen geschützt werden. Berücksichtigen Sie bei der Bestimmung der Sicherheitsstufe den zu sichernden Ressourcentyp.

Bei Verwendung von DIVArchive schützen Sie die folgenden Ressourcen:

2.1.1.1. Primärer Datenträger

Zum Erstellen von DIVArchive-Systemen sind Datenträger- und Cachedatenträger-Ressourcen vorhanden. Dies sind im Allgemeinen lokale und Remotedatenträger, die mit den DIVArchive-Systemen verbunden sind. Ein unabhängiger Zugriff auf diese Datenträger (nicht über DIVArchive) stellt ein Sicherheitsrisiko dar. Diese Form des externen Zugriffs kann von einem Rogue-System ausgehen, das von FC-Festplatten liest oder auf diese schreibt, oder von einem internen System, das unbeabsichtigt Zugriff auf diese Datenträger gewährt.

2.1.1.2. Datenbankdatenträger, Metadatendatenträger und Backupdatenträger

Mit Datenbankdatenträgern, Metadatendatenträgern und Backupdatenträgern können DIVArchive-Systeme mit komplexen Objekten erstellt werden. Dies sind im Allgemeinen **lokale oder Remotedatenträger**, die mit den DIVArchive-Systemen verbunden sind. Ein unabhängiger Zugriff auf diese Datenträger (nicht über DIVArchive) stellt ein Sicherheitsrisiko dar. Diese Form des externen Zugriffs kann von einem Rogue-System ausgehen, das von FC-Festplatten liest oder auf diese schreibt, oder von einem internen System, das unbeabsichtigt Zugriff auf diese Datenträger gewährt.

2.1.1.3. DIVArchive-Bänder

Der unabhängige Zugriff auf Bänder, insbesondere in einer Bandbibliothek, die von DIVArchive-Systemen kontrolliert wird, in die Daten geschrieben werden, stellt ein Sicherheitsrisiko dar.

2.1.1.4. Exportieren von Bandmetadaten

Dumps von Bandmetadaten, die mit Exportvorgängen erstellt werden, können Daten und Metadaten enthalten. Diese Daten und Metadaten sollten bei routinemäßigen Export- oder Importvorgängen nur BS-Administratoren zugänglich sein.

2.1.1.5. Konfigurationsdateien und Einstellungen

Einstellungen der DIVArchive-Systemkonfiguration müssen vor Nicht-Administratorbenutzern auf BS-Ebene geschützt werden. Im Allgemeinen werden diese Einstellungen automatisch von Benutzern mit Administratorberechtigungen auf BS-Ebene geschützt. Beachten Sie, dass ein Sicherheitsrisiko entsteht, wenn andere BS-Benutzer als der Administrator in Konfigurationsdateien schreiben können.

2.1.2. Vor wem werden die Ressourcen geschützt?

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

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 DIVArchive-Vorgängen nicht entsprechen) bis hin zu Datenbeschädigungen (Schreiben auf Datenträger oder Band außerhalb der normalen Berechtigungen) reichen.

2.2. Empfohlene Deployment-Topologien

In diesem Abschnitt wird beschrieben, wie eine Infrastrukturkomponente sicher installiert und konfiguriert wird. Weitere Informationen zur Installation von DIVArchive finden Sie in der DIVArchive Software Release 7.3 Customer Documentation Library unter:

<https://docs.oracle.com/en/storage/#csm>

Beachten Sie bei der Installation und Konfiguration von DIVArchive Folgendes:

2.2.1. Separates Metadatenetzwerk

Zur Verbindung zwischen DIVArchive-Servicekomponenten, Verbindung zur Metadatenbank und Verbindung von deren Clients stellen Sie ein separates TCP/IP-Netzwerk und eine Switch-Hardware bereit, die nicht mit einem WAN verbunden ist. Da der

Metadatenverkehr über TCP/IP implementiert wird, kann theoretisch ein externer Angriff erfolgen. Die Konfiguration eines separaten Metadatennetzwerks verringert dieses Risiko und sorgt zudem für eine bessere Leistung. Wenn kein separates Netzwerk erstellt werden kann, verweigern Sie wenigstens den Datenverkehr vom externen WAN und von allen nicht vertrauenswürdigen Hosts im Netzwerk zu den DIVArchive-Ports. Siehe [Abschnitt 1.2.2, „Netzwerkzugriff auf kritische Services begrenzen“](#).

2.2.2. FC-Zoning

Verwenden Sie FC-Zoning, um den Zugriff auf die DIVArchive-Datenträger abzulehnen, die über Fibre Channel von einem Server verbunden sind, der keinen Zugriff auf die Datenträger benötigt. Verwenden Sie einen separaten FC-Switch, um eine physische Verbindung nur mit den Servern herzustellen, die den Zugriff benötigen.

2.2.3. Absichern des Zugriffs auf SAN-Datenträgerkonfiguration

Auf SAN RAID-Datenträger kann im Allgemeinen zu administrativen Zwecken mit TCP/IP oder eher mit HTTP zugegriffen werden. Sie müssen die Festplatten vor externen Zugriffen schützen, indem Sie den Systemverwaltungszugriff auf SAN RAID-Festplatten auf vertrauenswürdige Domains beschränken. Ändern Sie außerdem das Standardpasswort auf den Festplattenarrays.

2.2.4. Installieren des DIVArchive-Packages

Erstens, installieren Sie nur die DIVArchive-Services, die Sie benötigen. Beispiel: Wenn Sie die grafische Benutzeroberfläche oder das Konfigurationsdienstprogramm in einem System nicht verwenden möchten, heben Sie die entsprechende Auswahl in der Liste der zu installierenden Komponenten auf. Die Standardberechtigungen und Eigentümer des DIVArchive-Installationsverzeichnis sollten nach der Installation nicht ohne vorherige gründliche Überlegung der Auswirkungen auf die Sicherheit geändert werden.

2.2.5. DIVArchive-Bandsicherheit

Verhindern Sie den externen Zugriff auf DIVArchive-Bänder innerhalb der Bandbibliothek, die von dem DIVArchive-System kontrolliert wird. Durch den unberechtigten Zugriff auf DIVArchive-Bänder können Benutzerdaten beschädigt oder gelöscht werden.

2.2.6. Backups

Mit dem DIVArchive Backup Service können Sie Datenbankbackups einrichten und durchführen. Begrenzen Sie den Zugriff auf den Backupdump nur auf Administratorbenutzer auf BS-Ebene.

2.3. Konfiguration nach Abschluss der Installation

Gehen Sie nach der Installation von DIVArchive durch die Sicherheitsprüfliste in [Anhang A, Prüfliste für sicheres Deployment](#).

Kapitel 3. Sicherheitsfunktionen

Um potenzielle Sicherheitsrisiken zu vermeiden, müssen sich Kunden, die DIVArchive verwenden, um Authentifizierung und Autorisierung des Systems kümmern.

Diese Sicherheitsrisiken können durch ordnungsgemäße Konfiguration und Befolgen der Prüfliste nach Abschluss der Installation in [Anhang A, Prüfliste für sicheres Deployment](#) minimiert werden.

3.1. Sicherheitsmodell

Die folgenden kritischen Sicherheitsfunktionen bieten Schutz vor Sicherheitslücken:

- Authentifizierung - Sie stellt sicher, 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.

3.2. Authentifizierung

Die grafische DIVArchive-Kontrollbenutzeroberfläche stellt drei feste Benutzerprofile bereit (Administrator, Operator und Benutzer). Für den Zugriff auf die Administrator- und Operatorkonten ist ein Passwort erforderlich. In dem DIVArchive-System sind bereits Standardpasswörter installiert, die jederzeit über das DIVArchive-Konfigurationsdienstprogramm geändert werden können. Wenn die Standardpasswörter nicht geändert werden, ist das DIVArchive-System für böswillige Aktivitäten anfällig. **Standardpasswörter müssen sofort nach der Installation und Konfiguration der Administrator- und Operatorkonten und danach (mindestens) alle 180 Tage geändert werden. Nachdem die Änderung vorgenommen wurde, müssen Sie die Passwörter an einem sicheren Ort, offline, aufbewahren, damit sie gegebenenfalls Oracle Support zur Verfügung gestellt werden können.**

3.3. Zugriffskontrolle

Die Zugriffskontrolle in DIVArchive ist in drei Profile unterteilt:

Benutzer - Nachdem die Verbindung zu DIVArchive Manager hergestellt wurde, lässt die grafische Kontrollbenutzeroberfläche nur zu, dass der Benutzer DIVArchive-Vorgänge

überwacht und Daten aus der Datenbank abrufen. Dies wird als Benutzerprofil bezeichnet. Im Benutzerprofilmodus kann nicht auf alle Funktionen zugegriffen werden, die Befehle an DIVArchive absetzen. Dies kann zu Fällen führen, bei denen eine Überwachung erforderlich ist, jedoch keine Befehle an DIVArchive gesendet werden dürfen.

Administrator - Um Anforderungen an DIVArchive zu stellen, wie Anforderungen zur Archivierung oder Wiederherstellung oder zum Auswerfen eines Bandes aus der Bibliothek müssen Sie zum Administratorprofil wechseln. Das Administratorprofil ist passwortgeschützt. Das Standardpasswort für dieses Profil ist diva, dies kann jedoch im Konfigurationsdienstprogramm geändert werden (oder geändert worden sein). Weitere Informationen finden Sie in der DIVArchive Software Release 7.3 Customer Documentation Library unter:

<https://docs.oracle.com/en/storage/#csm>

Operator - Neben den Berechtigungen des Benutzerprofils ermöglicht das Operatorprofil Zugriff auf das Objektübertragungsprogramm und erfordert die Eingabe desselben Passwortes wie für das Administratorprofil.

Anhang A. Prüfliste für sicheres Deployment

1. Legen Sie sichere Passwörter für Administrator- und andere BS-Konten fest, denen DIVArchive-Administrator-oder -Servicerollen zugewiesen sind, einschließlich:
 - DIVA, Oracle-Benutzer-IDs (sofern verwendet)
 - Verwaltungskonten im Festplattenarray
2. Verwenden Sie kein lokales Administrator-BS-Konto, sondern weisen Sie anderen Benutzerkonten Rollen nach Bedarf zu.
3. Legen Sie ein sicheres Passwort für Administrator und Operator der grafischen Kontrollbenutzeroberfläche fest. Ändern Sie das Passwort sofort von dem bei der Installation festgelegten Standardpasswort in ein sicheres Passwort. Dazu können Sie das Konfigurationsdienstprogramm unter "Tools" verwenden.
4. Legen Sie ein sicheres Passwort für die Oracle-Datenbankanmeldung fest, Ändern Sie die bei der Installation festgelegten Standardpasswörter für Oracle-Datenbankbenutzer.
5. Installieren Sie eine Firewall auf jedem System, und wenden Sie die Standardregeln für DIVArchive-Ports an. Begrenzen Sie den Zugriff auf die DIVArchive-API (TCP 9000) auf IPs, die Zugriff benötigen, mit Firewall-Regeln.
6. Installieren Sie regelmäßig BS- und DIVArchive-Updates, weil diese Sicherheitsupdates umfassen.
7. Installieren Sie einen Virenschutz, und schließen Sie die DIVArchive-Prozesse und -Speicherung aus Performancegründen aus.
8. Als Best Practice wird empfohlen, FC-Datenträger und FC-Bandlaufwerke entweder physisch oder durch FC-Zoning zu trennen, sodass Datenträger und Bandgeräte nicht denselben HBA-Port verwenden. Bei verwalteten Datenträgern sollten nur DIVArchive Actor Zugriff auf den Datenträger und auch die Bandlaufwerke haben. Durch diese Sicherheitsmaßnahme wird verhindert, dass Zwischenfälle aufgrund von Datenverlust als Folge von unabsichtlichem Überschreiben von Bändern oder Festplatten auftreten.
9. Richten Sie ein entsprechendes Backupset der DIVArchive-Konfiguration und -Datenbank ein. Mithilfe von Backups, die Teil eines Sicherheitskonzepts sind, können Daten, die unabsichtlich oder durch Unbefugte gelöscht wurden, wiederhergestellt werden. Ihr Backup sollte richtlinienkonform sein, wenn es an einem anderen Speicherort abgelegt wird. Backups müssen in demselben Maße wie DIVARrchive-Bänder und -Festplatten geschützt werden.
