Oracle® DIVArchive

Sicherheitshandbuch

Release 7.5

E86534-01

November 2016

ORACLE

Oracle® DIVArchive
Sicherheitshandbuch

E86534-01

Inhalt

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.

1

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. Oracle DIVArchive Manager

DIVArchive Manager ist die Hauptkomponente in einem DIVArchive-System. Alle Archivierungsvorgänge werden vom DIVArchive Manager kontrolliert und verarbeitet. Vorgangsanforderungen 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 7.4 Customer Documentation Library unter:

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

1.1.2. Oracle 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 einen 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 Release 7.4 Customer Documentation Library unter:

`https://docs.oracle.com/en/storage/#csm`

1.1.5. Oracle DIVArchive 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 (DFM)

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. DIVArchive SNMP wird nur in Windows-Umgebungen unterstützt.

1.1.8. DIVArchive Storage Plan Manager (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 können Sie Vorgänge in DIVArchive überwachen, kontrollieren und beaufsichtigen. Verschiedene grafische DIVArchive-Benutzeroberflächen können gleichzeitig ausgeführt und mit demselben DIVArchive-System verbunden werden.

1.1.12. DIVArchive-Konfigurationsdienstprogramm

Mit dem DIVArchive-Konfigurationsdienstprogramm können Sie ein DIVArchive-System konfigurieren. 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 Local Delete

Local Delete ist ein Service, der Funktionen der Objektreplikation zwischen einem lokalen DIVArchive-System (z.B. DIVAlocal) und einem (oder mehreren) Remote-DIVArchive-Systemen (z.B. DIVAdr) 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 immer auf dem neuesten Stand halten

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:

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

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

Führen Sie DIVArchive-Services nicht mit einem Administrator- (oder Root-)Betriebssystembenutzerkonto aus. Sie müssen alle DIVArchive-Services immer mit einem dedizierten Betriebssystembenutzer (oder einer BS-Gruppe) namens DIVA ausführen.

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. Vor der Verwendung dieser Profile müssen Sie ein Administrator- und/oder Operatorpasswort im Konfigurationsdienstprogramm zuweisen.

Sie erstellen Passwörter während der Installation und Konfiguration sowohl für Administrator- als auch für Operatorkonten. Die Passwörter müssen danach (mindestens) alle 180 Tage geändert werden. Passwörter müssen falls erforderlich Oracle Support verfügbar gemacht werden.

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.

2

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. Analysieren der Umgebung

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 Cachedatenträgerressourcen vorhanden. Dies sind im Allgemeinen lokale und Remote-Datenträger, die mit den DIVArchive-Systemen verbunden sind. Der unabhängige Zugriff auf diese Datenträger (außer durch 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 und Remote-Datenträger, die mit den DIVArchive-Systemen verbunden sind. Der unabhängige Zugriff auf diese Datenträger (außer durch 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 Metadatenberechtigungen müssen ausschließlich auf das Administrator- (oder Root-)Betriebssystemkonto oder den DIVA-Betriebssystembenutzer (bzw. die BS-Gruppe) während einer routinemäßigen Export- oder Importaktivität begrenzt sein.

2.1.1.5. Konfigurationsdateien und Einstellungen

Die Konfigurationseinstellungen des DIVArchive-Systems müssen vor Betriebssystembenutzern ohne Administratorrechte geschützt werden. Wenn Schreibzugriff auf die Konfigurationsdateien für Betriebssystembenutzer ohne Administratorrechte erteilt wird, stellt dies ein Sicherheitsrisiko dar. Deshalb müssen diese Dateiberechtigungen ausschließlich auf das Administrator- (oder Root-)Betriebssystemkonto oder den DIVA-Betriebssystembenutzer (bzw. die BS-Gruppe) begrenzt sein.

2.1.2. Vor wem werden die Ressourcen geschützt?

Im Allgemeinen müssen die auf einem konfigurierten System im vorherigen Abschnitt beschriebenen Ressourcen vor sämtlichen Zugriffen geschützt werden. Dazu gehören auch Zugriffe aus externen Rogue-Systemen 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 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 7.4 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 Metadatennetzwerk

Zur Verbindung zwischen DIVArchive-Servicekomponenten, Verbindung zur Metadatendatenbank 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 Netzwerkzugriff auf kritische Services begrenzen.

2.2.2. FC-Zoning

Verweigern Sie mit FC-Zoning den Zugriff auf die DIVArchive-Datenträger, die über Fibre Channel an Server angeschlossen sind, die keinen Zugriff auf die Datenträger benötigen. 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 Berechtigungen und die Eigentümer des Standard-DIVArchive-Installationsverzeichnisses müssen ausschließlich auf das Administrator- (oder Root-)Konto oder den DIVA-Betriebssystembenutzer (bzw. die BS-Gruppe) begrenzt sein.

2.2.5. DIVArchive-Bandsicherheit

Verhindern Sie den externen Zugriff auf DIVArchive-Bänder innerhalb einer Bandbibliothek, die vom 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. Berechtigungen für den Backupdump müssen ausschließlich auf das Administrator- (oder Root-)Betriebssystemkonto oder den DIVA-Betriebssystembenutzer (bzw. die BS-Gruppe) begrenzt sein.

2.3. Konfiguration nach Abschluss der Installation

Gehen Sie nach der Installation von DIVArchive durch die Sicherheitsprüfliste in Anhang A, *Prüfliste für sicheres Deployment*.

3

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. Vor der Verwendung dieser Profile müssen Sie ein Administrator- und/oder Operatorpasswort im Konfigurationsdienstprogramm zuweisen.

Die Passwörter für Administrator- und Operatorkonten müssen (mindestens) alle 180 Tage geändert werden. Passwörter müssen falls erforderlich Oracle Support verfügbar gemacht werden.

3.3. Zugriffskontrolle

Die Zugriffskontrolle in DIVArchive ist in drei Profile unterteilt. Für den Zugriff auf die Administrator- und Operatorkonten ist ein Passwort erforderlich. Vor der Verwendung dieser Profile müssen Sie ein Passwort für Administrator- und/oder Operatorkonten im Konfigurationsdienstprogramm zuweisen.

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 abruft. Dies wird als Benutzerprofil bezeichnet. Nicht alle Funktionen, die Befehle an DIVArchive ausgeben, können im Benutzerprofilmodus aufgerufen werden, sodass es zu Situationen kommen kann, bei denen eine Überwachung erforderlich ist, jedoch keine Befehle an DIVArchive gesendet werden können.

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 Passwort für dieses Profil muss vor Verwendung des Profils im Konfigurationsdienstprogramm zugewiesen werden. Weitere Informationen finden Sie in der Oracle DIVArchive 7.4 Customer Documentation Library unter:

`https://docs.oracle.com/en/storage/#csm`

Operator und *Erweiterter Operator* - Neben den Benutzerprofilberechtigungen ermöglicht das Operatorprofil Zugriff auf das Objektübertragungsdienstprogramm. Dazu muss vor Verwendung des Profils ein Passwort im Konfigurationsdienstprogramm konfiguriert werden. Mit den Profilen "Operator" und "Erweiterter Operator" können auf der grafischen Kontrollbenutzeroberfläche Berechtigungen zum Abbrechen oder Ändern von Prioritätsanforderungen optional aktiviert werden. Die Optionen sind im Bereich für die Manager-Konfiguration des Konfigurationsdienstprogramms definiert. Standardmäßig ist diese Option *deaktiviert*.

Anhang A

Anhang A. Prüfliste für sicheres Deployment

1. Legen Sie sichere Passwörter für Administrator- (oder Root-) und andere Betriebssystemkonten fest, denen DIVArchive-Administrator-oder -Servicerollen zugewiesen sind, einschließlich:
   - DIVA, Oracle-Benutzer-IDs (sofern verwendet)
   - Verwaltungskonten im Festplattenarray
2. Verwenden Sie kein lokales Administratorbetriebssystemkonto. Weisen Sie anderen Benutzerkonten nach Bedarf Rollen zu.
3. Legen Sie ein sicheres Passwort für Administrator und Operator der grafischen Kontrollbenutzeroberfläche fest. Sie müssen diesen Profilen vor der Verwendung ein Passwort im Konfigurationsdienstprogramm zuweisen.
4. Legen Sie ein sicheres Passwort für die Anmeldung bei der Oracle-Datenbank fest.
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 Betriebssystem- 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 dürfen nur DIVArchive Actor Zugriff auf den Datenträger und 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.