Oracle® DIVAnet

Sicherheitshandbuch

Release 2.1

E77638-01

Juni 2016

ORACLE®

Oracle® DIVAnet
Sicherheitshandbuch

E77638-01

Inhalt

Vorwort

Das Oracle DIVAnet - Sicherheitshandbuch beinhaltet Informationen zum Oracle DIVAnet-Produkt und erläutert die allgemeinen Prinzipien der Anwendungssicherheit.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung der Sicherheitsfunktionen und der sicheren Installation und Konfiguration von DIVAnet 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 Oracle DIVAnet 2.1 und Erläuterungen allgemeiner Grundsätze sicherer Anwendungen.

1.1. Produktüberblick

Oracle DIVAnet bietet einen einheitlichen Überblick über archivierte Inhalte auf mehreren, verteilten Oracle DIVArchive-Systemen. Oracle DIVArchive ist ein skalierbares Content Storage Management-System, das die Archivierung in Bandbibliotheken und Datenträgersystemen unterstützt. DIVAnet ermöglicht ein einfaches Verschieben von Inhalten zwischen DIVArchive-Sites und von Quell- und Zielservern und -datenträgern von Kunden. Es führt Aufgaben in den Bereichen Disaster Recovery, Verteilung von Inhalten, Zugriffskontrolle, Performance und Inhaltsverfügbarkeit aus.

DIVAnet besteht aus den folgenden Hauptkomponenten:

1.1.1. DIVAnet ClientAdapter Service

Anwendungsclients, die die DIVArchive-API oder die DIVAnet-GUI verwenden möchten, bauen eine Verbindung zum **DIVAnet ClientAdapter Service** auf. Dieser DIVAnet-Service akzeptiert Web- und Socket-Verbindungen von Anwendungen und verarbeitet die Anforderungen. Ein **ClientAdapter** wird auf jeder Site konfiguriert, auf der Anwendungen ausgeführt werden, die sich lokal auf der Site mit DIVArchive- und DIVAnet-Installationen befinden.

1.1.2. DIVAnet ManagerAdapter Service

Der **DIVAnet ManagerAdapter Service** dient als Brücke zwischen DIVAnet und Oracle DIVArchive Manager. Er muss konfiguriert werden, um anderen DIVAnet-Systemen Remote-Zugriff zu ermöglichen.

1.1.3. DIVAnet DbSync Service

Der **DIVAnet DbSync Service** ist dafür zuständig, Assetinformationen aus mehreren DIVArchive-Sites zu synchronisieren und die Informationen in der DIVAnet-Datenbank zu speichern. **DbSync** führt eine Remote-Kommunikation mit **ManagerAdapter**-Services

auf mehreren Sites durch, um Informationen zu archivierten Objekten zu synchronisieren. **DbSync** wird in der Regel zusammen mit dem **ClientAdapter** bereitgestellt. Sowohl der **DbSync**-Service als auch der **ClientAdapter** benötigen Direktzugriff auf die DIVAnet-Datenbank.

1.1.4. DIVAnet-Benutzeroberfläche (DIVAnetUI)

DIVAnetUI ist eine GUI-Anwendung, mit der Benutzer DIVAnet-Anforderungen überwachen sowie DIVAnet-Assets (archivierte DIVA-Objekte) auf mehreren DIVArchive-Sites anzeigen, kopieren und löschen können. Alle Anforderungen auf DIVAnet-Ebene können überwacht werden, unabhängig davon, ob sie über die API oder über die UI selbst ausgegeben wurden. Sie können auch Assetinformationen für alle konfigurierten DIVArchive-Sites anzeigen, unabhängig davon, ob das Asset über DIVAnet archiviert wurde. **DIVAnetUI** bietet flexible Möglichkeiten zur Abfrage von sowohl Anforderungs- als auch Assetinformationen.

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

Die DIVAnet-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 muss auf kritische Services begrenzt sein

Standardmäßig verwendet DIVAnet die folgenden TCP/IP-Ports:

- *`tcp/9801`* ist der Standard-**WebService**-Port, der von DIVAnet **ClientAdapter** verwendet wird
- *`tcp/7101`* ist der Standard-API-Socket-Port, der von DIVAnet **ClientAdapter** verwendet wird (Sie können andere Ports konfigurieren)
- *`tcp/9800`* ist der Standard-**WebService**-Port, der von DIVAnet **ManagerAdapter** verwendet wird

Hinweis:

Diese Ports müssen nicht alle für einen externen Zugriff zugänglich gemacht werden und basieren auf Konfiguration und Verwendung.

1.2.3. Wenn möglich, muss das Prinzip der niedrigsten Berechtigungsstufe verwendet werden

DIVAnet-Services dürfen nicht als *admin* oder *root* ausgeführt werden. Führen Sie die Services als ein anderer Betriebssystembenutzer (und nicht als Administratorbenutzer der Anwendung) aus, um die Gesamtsicherheit des Systems zu erhöhen.

Das DIVanet Linux-Installationsprogramm erfordert zwei Benutzer, um die DIVAnet-Installation abzuschließen - *diva* und einen Betriebssystembenutzer. Administratoren und Operatoren verwenden das *diva*-Konto zur Installation und Überwachung von DIVAnet. Der Betriebssystembenutzer kontrolliert die DIVAnet-Services.

Firewalls müssen den Portzugriff weitestgehend einschränken. DIVAnet umfasst Funktionen zur Zugriffskontrolle (kurz in Zugriffskontrolle erläutert), mit denen Benutzer und Systeme auf die jeweils niedrigstmögliche Berechtigungsstufe beschränkt werden.

1.2.4. Überwachen der Systemaktivität

Sie müssen die Systemaktivität überwachen, um festzustellen, wie gut DIVAnet arbeitet und ob ungewöhnliche Aktivitäten protokolliert werden. Prüfen Sie die Protokolldateien im Ordner *$DIVANET_HOME/Program/log/*.

1.2.5. Sicherheitsinformationen immer auf dem neuesten Stand halten

Unter folgender Adresse haben Sie Zugriff auf mehrere Quellen mit Sicherheitsinformationen und Alerts für eine Vielzahl an Softwareprodukten:

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

Sie bleiben hinsichtlich der Sicherheit vor allem dann auf dem neuesten Stand, wenn Sie das neueste Release der DIVAnet-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 Production-Umgebung können zahlreiche Ressourcen geschützt werden. Berücksichtigen Sie bei der Bestimmung der Sicherheitsstufe den zu sichernden Ressourcentyp.

Bei der Verwendung von DIVAnet müssen folgende Ressourcen geschützt werden:

2.1.1.1. DIVAnet-Server

DIVAnet wird auf einem Server installiert, der mit mindestens einem Datenträger (entweder einem lokalen oder einem direkt mit dem DIVAnet-System verbundenen Remote-Datenträger) verknüpft ist. Ein unabhängiger Zugriff auf diese Datenträger (nicht über DIVAnet) 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. Datenbank

Zum Aufbau von DIVAnet-Systemen werden Datenbanksoftware und Datenressourcen verwendet. Die Daten werden in der Regel auf lokalen oder Remote-Datenträgern vorgehalten, die mit den DIVAnet-Systemen verbunden sind. Ein unabhängiger Zugriff auf diese Datenträger (nicht über DIVAnet) 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. DIVArchive-Quellen, -Ziele und Archivmedien

DIVAnet verwendet DIVArchive-Quellen und -Ziele sowie DIVA-Archivierungssysteme (Datenträger oder Band) zur Verarbeitung von Anforderungen. Unbefugter unabhängiger Zugriff auf diese Serverdatenträger und Systemmedien, die in der Regel durch DIVArchive-Systeme gesteuert werden, stellt ein Sicherheitsrisiko dar. Die **Quellen/Ziele**, die als temporäre Datenspeicher für DIVAnet-Kopiervorgänge verwendet werden, müssen zugriffsbeschränkt sein. Sie sollten diese **Quellen/Ziele** ausschließlich für DIVAnet-Vorgänge reservieren und außerdem sicherstellen, dass Übertragungen verschlüsselt oder über ein vertrauenswürdiges Netzwerk initiiert werden.

2.1.1.4. Konfigurationsdateien und Einstellungen

Die Konfigurationseinstellungen des DIVAnet-Systems müssen vor Betriebssystembenutzern ohne Administratorrechte geschützt werden. Im Allgemeinen werden diese Einstellungen automatisch von Betriebssystembenutzern mit Administratorrechten geschützt. Es entsteht ein Sicherheitsrisiko, wenn andere Betriebssystembenutzer als der Administrator in Konfigurationsdateien schreiben können.

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 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 nicht den normalen DIVAdirector-Vorgängen entsprechen) bis hin zu Datenbeschädigungen (versehentliches Löschen von Assets oder Schreiben auf Datenträger oder Band außerhalb der normalen Berechtigungen) reichen.

2.2. Empfohlene Deployment-Technologien

In diesem Abschnitt werden Installation und Konfiguration einer sicheren Infrastrukturkomponente beschrieben.

Informationen zur Installation von DIVAnet finden Sie in *Oracle DIVAnet - Installations-, Konfigurations- und Betriebshandbuch* in der *DIVAnet 2.1-Dokumentationsbibliothek* unter:

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

Beachten Sie bei der Installation und Konfiguration von DIVAnet Folgendes.

2.2.1. DIVAnet-Installation

Installieren Sie nur die DIVAnet-Komponenten, die Sie benötigen. Beispiel: Wenn Sie von einem Clientcomputer nur **DIVAnetUI** ausführen möchten, deaktivieren Sie die Option **DIVAnet Services** in der Liste der zu installierenden Komponenten. Die Standardberechtigungen und Eigentümer des DIVAnet-Installationsverzeichnisses dürfen nach der Installation nicht ohne vorherige gründliche Überlegung der Auswirkungen auf die Sicherheit geändert werden.

2.2.2. Verbinden mit DIVArchive

Oracle empfiehlt, zur Erhöhung der Systemsicherheit die Installation der **ManagerAdapter**-Komponente auf dem DIVArchive Manager-System. Wird kein externer Zugriff auf den DIVArchive Manager-Port benötigt, wird empfohlen, den Port über Firewallsoftware zu blockieren. Darüber hinaus ist es oft unnötig, einen externen Netzwerkzugriff auf den **DIVAnet DbSync WebService**-Port zu gestatten.

Wenn Sie eine Verbindung zu einer Remote-DIVArchive-Instanz über ein WAN herstellen, achten Sie darauf, die Verbindung über ein vertrauenswürdiges Netzwerk aufzubauen. Außerdem sollten Sie die Site über `SSL/TLS` mit dem **ManagerAdapter**-Port der Remote-Site verbinden.

2.2.3. Schützen von Datenträgersystemen

Verweigern Sie mit FC-Zoning den Zugriff auf die DIVAnet-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.

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

2.3. Konfiguration nach Abschluss der Installation

Gehen Sie nach jeder Installation von DIVAnet-Komponenten durch die Prüfliste für sicheres Deployment in Anhang A, *Prüfliste für sicheres Deployment*.

3

Kapitel 3. Sicherheitsfunktionen

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

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 -** 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.

3.2. Authentifizierung

DIVAnet-Services können über mehrere Methoden eine Authentifizierung ausführen:

- **SSL/TLS-Zertifikate** - Beim Herstellen einer ausgehenden Verbindung zu einem Remote-DIVAnet-Service konsultiert DIVAnet einen Zertifikats-Truststore. Dadurch wird sichergestellt, dass DIVAnet eine Verbindung zu authentischen DIVAnet-Services herstellt. Um eine sichere Verbindung vom DIVAnet **ClientAdapter** zu einer DIVArchive-Instanz aufzubauen, müssen Sie die Verbindung über den **ManagerAdapter** mit einem `<ConnectionType>` herstellen, der als **WebServices** identifiziert wird.
- **Zugriffsregeln** - Zugriffsregeln, die streng genommen eine Art der Zugriffskontrolle darstellen, können eingehende Verbindungen anhand der eingehenden IP-Adressen filtern. Diese Funktion ist erforderlich, um sicherzustellen, dass nur zugelassene Systeme entsprechenden Zugriff auf DIVAnet-Services erhalten.

WARNUNG:

DIVAnet-Services verwenden Datenbankpasswörter als Teil ihrer Konfiguration. Passwörter müssen umgehend nach der Installation und danach (mindestens) alle 180 Tage geändert werden. Nach der Änderung müssen Sie die Passwörter an einem sicheren Ort offline aufbewahren und Oracle Support bei Bedarf vorlegen können.

3.3. Zugriffskontrolle

Mit Zugriffsregeln können Sie die Vorgänge einschränken, die bestimmte Benutzer oder Systeme im verteilten Archivsystem ausführen dürfen. Zugriffsregeln können auf folgende Arten ausgeführt werden:

- **ClientAdapter-/MultiDiva-Modus** - Schränkt ein, welche Arten von DIVAnet-Anforderungen ausgeführt werden können.
- **ManagerAdapter** - Schränkt ein, welche Arten von DIVArchive-Anforderungen zur Erfüllung einer DIVAnet-Anforderung (möglicherweise von einem Remote-System) ausgeführt werden können.

Zugriffsregeln können sich auf Anforderungen auswirken, die über die **DIVAnetUI** oder über eine API-Socket-Verbindung (möglicherweise über ein MAM- oder Automatisierungssystem) ausgelöst wurden.

Für eine DIVAnet-Anforderung können Zugriffsregeln auf DIVAnet-Ebene oder auf DIVArchive-Ebene ausgeführt werden. Auf DIVAnet-Ebene verarbeitet der **ClientAdapter** die Anforderung dort, wo sie empfangen wurde. Auf DIVArchive-Ebene verarbeitet ein Remote-**ManagerAdapter** DIVArchive-Anforderungen, die zur Erfüllung der DIVAnet-Anforderung ausgegeben werden.

Oracle empfiehlt, einen Satz Regeln mit den für die Erfüllung Ihrer Anwendungsanforderungen größtmöglichen Einschränkungen zu erstellen. Beispiel: Wenn globale Löschvorgänge nur von Administratoren ausgeführt werden müssen, stellen Sie sicher, dass anderen Benutzern der Zugriff auf diese Funktionalität verweigert wird. Wenn eine Gruppe von Systembenutzern nur Zugriff auf eine begrenzte Liste von Quellen und Zielen benötigt, stellen Sie sicher, dass diese Benutzer nur Anforderungen zu diesen jeweiligen Quellen und Zielen ausgeben können.

Überlegen Sie auch, welche Sites zur Erfüllung von Anforderungen benötigt werden. Beispiel: Wenn Benutzer auf der lokalen Site keinen Grund haben, Kopiervorgänge vorzunehmen, bei denen weder die Quell- noch die Zielsite die lokale Site sind (dies ist mit DIVAnet möglich), konfigurieren Sie diese Regeln in der **ClientAdapter**-Konfiguration.

Erwägen Sie auch bestimmte Konstrukte in Anforderungen, die Sie generell ausschließen möchten. Beispiel: Wenn Objekte nicht nur mit dem Objektnamen (ohne Kategorie) adressiert werden müssen, schließen Sie alle Anforderungen aus, bei denen die Kategorie nicht angegeben ist.

Darüber hinaus enthält jedes ClientAdapter WorkflowProfile die Liste gültiger Nachrichten, die durch Anforderungen, die dem WorkflowProfile zugewiesen sind, verarbeitet werden können. Im **MultiDiva-Modus** können Sie dadurch bestimmte Nachrichten von der Verarbeitung ausschließen (einschließlich Informationsnachrichten).

Oracle empfiehlt, zu Anfang die in der Datei *`AccessRules.xml.ini`* definierten Standardregeln zu verwenden, auch wenn Sie keine eigenen Zugriffsregeln definieren.

Weitere Informationen zu den DIVAnet-Zugriffskontrollfunktionen finden Sie im *Oracle DIVAnet - Installations-, Konfigurations- und Betriebshandbuch* unter:

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

3.4. Konfigurieren von SSL/TLS

DIVAnet enthält an zwei Stellen Zertifikatdaten: in einem *privaten Keystore*, der für auf dem lokalen System gehostete Webservices verwendet wird, und in einem *öffentlichen Keystore*, mit dem per Remote-Zugriff aufgerufene Webservices verifiziert werden. Mit dem **Java Keytool-Dienstprogramm** können Sie das Passwort des Keystores ändern und Zertifikate hinzufügen und löschen.

Weitere Informationen zum Erstellen von Keystores finden Sie unter:

http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#CreateKeystore

Nur die DIVAnet-Webservicesverbindungen verwenden *SSL/TLS*. In diesem Release wird für Verbindungen zu DIVArchive oder DIVAnet über eine DIVArchive-API-Socket-Verbindung nicht *SSL/TLS* verwendet.

3.4.1. Privater Keystore

Private Key-Daten zu DIVAnet-Zertifikaten werden gespeichert in:

$DIVANET_HOME/Program/divanet/lib/diva129.jks

In diesem Keystore muss genau ein Zertifikat enthalten sein. Dieses Zertifikat wird für Webservices verwendet, die von Services gehostet werden, die über dieses *$DIVANET_HOME*-Verzeichnis ausgeführt werden. Es wird empfohlen, das mitgelieferte Zertifikat durch ein neues Zertifikat zu ersetzen und für jede DIVAnet-Site in Ihrem Netzwerk ein eigenes Zertifikat zu verwenden.

Sie müssen das Passwort dieses Keystores ändern. Speichern Sie die Passwortinformationen in einer neuen Datei namens *$DIVANET_HOME/Program/divanet/lib/diva129.properties*, und machen Sie diese Datei für DIVAnet-Services (in Linux ist dieser Benutzer *divanetsvc*), jedoch nicht für gelegentliche Benutzer des Systems (z.B. den *diva*-Benutzer in Linux) lesbar. Verwenden Sie folgendes Format für die Datei:

keystorePassword=newpassword

3.4.2. Öffentlicher Keystore

Diese gelegentlich auch als *Truststore* bezeichneten Daten befinden sich in:

$DIVANET_HOME/Java/lib/security/cacerts2

Diese Zertifikatdaten werden in ausgehenden Webserviceaufrufen (einschließlich **DIVAnetUI**) verwendet. In diesen Keystore können mehrere Public Keys geladen werden.

Wenn Sie zum privaten DIVAnet Keystore ein neues selbstsigniertes Zertifikat hinzugefügt haben, exportieren Sie das Zertifikat mit dem Keytool-Dienstprogramm. Alle Anwendungen (DIVAnet-Services, DIVAnetUI usw.), die auf dieser Site **WebServices** aufrufen, müssen das exportierte Zertifikat dann in ihren eigenen öffentlichen Keystore aufnehmen.

Anhang A

Anhang A. Prüfliste für sicheres Deployment

1. Legen Sie starke Passwörter für den Administrator sowie für alle weiteren Betriebssystemkonten fest, denen DIVAnet-Administrator- oder Servicerollen zugewiesen sind. Dies umfasst:
   - *`diva`*, *`divanetsvc`* und Oracle-Benutzer-IDs sofern verwendet
   - Alle Verwaltungskonten auf dem Datenträger
2. Verwenden Sie kein Betriebssystemkonto eines lokalen Administrators. Weisen Sie stattdessen anderen Benutzerkonten Rollen nach Bedarf zu.
3. Verwenden Sie für jede DIVAnet-Installation websitespezifische Zertifikate, und definieren Sie ein starkes Passwort für die Oracle-Datenbank und den privaten Keystore. Legen Sie ein starkes Passwort für die Anmeldung beim Oracle-Datenbankbetriebssystem fest.
4. Installieren Sie auf allen DIVAnet-Systemen Firewallsoftware, und wenden Sie die DIVAnet-Standardportregeln an. Schränken Sie den Zugriff auf das DIVAnet API-Socket (*`tcp 7101`*) auf IPs ein, für die ein Zugriff über Firewallregeln erforderlich ist. Führen Sie diesen Schritt mit den DIVAnet-Zugriffsregeln aus.
5. Installieren Sie Betriebssystem- und DIVAnet-Updates in regelmäßigen Abständen, da diese Sicherheitspatches enthalten.
6. Installieren Sie ein Antivirenprogramm, und schließen Sie die DIVAdirector-Prozesse und -Speicherung aus Performancegründen aus.
7. Best Practices schreiben eine Trennung von FC-Datenträgern und FC-Bandlaufwerken entweder physisch oder durch FC-Zoning vor, sodass Datenträger und Bandgeräte nicht denselben HBA-Port verwenden. Durch diese Sicherheitsmethode wird ein versehentliches Überschreiben wichtiger Daten verhindert.
8. Konfigurieren Sie eine angemessene Reihe von Backups für die DIVAnet-Konfiguration und Datenbank. 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 DIVAnet-Datenträger gesichert werden.