Oracle® DIVAnet

Security Guide

Release 2.1

E74486-01

June 2016

ORACLE®

Oracle DIVAnet Security Guide, Release 2.1

E74486-01

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Lou Bonaventura

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface v

Audience v
Documentation Accessibility v

1 Overview

Product Overview 1-1
DIVAnet ClientAdapter Service 1-1
DIVAnet ManagerAdapter Service 1-1
DIVAnet DbSync Service 1-1
DIVAnet User Interface (DIVAnetUI) 1-1
General Security Principles 1-2
Keep Software up to Date 1-2
Restrict Network Access to Critical Services 1-2
Use Principle of Least Privilege where Possible 1-2
Monitor System Activity 1-2
Keep Up To Date on Latest Security Information 1-2

2 Secure Installation

Understand Your Environment 2-1
Which resources need to be protected? 2-1
DIVAnet Servers 2-1
Database 2-1
DIVArchive Sources, Destinations, and Archive Media 2-1
Configuration Files and Settings 2-2
From whom are the resources being protected? 2-2
What will happen if the protections on strategic resources fail? 2-2
Recommended Deployment Technologies 2-2
DIVAnet Installation 2-2
Connecting to DIVArchive 2-2
Safeguard Disk Systems 2-2
Postinstallation Configuration 2-3

3 Security Features

The Security Model 3-1
Authentication 3-1

Access Control 3-2
Configuring SSL/TLS 3-2
Private Keystore 3-3
Public Keystore 3-3

A Secure Deployment Checklist

Preface

Oracle's DIVAnet Security Guide includes information about the Oracle DIVAnet product and explains the general principles of application security.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of DIVAnet.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Overview

This chapter provides an overview of the Oracle DIVAnet 2.1 product and explains the general principles of application security.

Product Overview

Oracle DIVAnet provides a unified view of archived content across multiple, distributed Oracle DIVArchive systems. Oracle's DIVArchive is a scalable content storage management system supporting archival to tape libraries and disk systems. DIVAnet facilitates the moving of content back and forth among DIVArchive sites, and from customer Source and Destination servers and disks. It performs its tasks for the purposes of disaster recovery, content distribution, access control, performance, and content availability.

DIVAnet consists of the following major components:

DIVAnet ClientAdapter Service

Application clients that want to use the DIVArchive API, or want to use the DIVAnet GUI, connect to the DIVAnet ClientAdapter Service. This DIVAnet service accepts web and socket connections from applications and processes the requests. A ClientAdapter is configured on each site that has applications that are local to the site where DIVArchive and DIVAnet are installed.

DIVAnet ManagerAdapter Service

The DIVAnet ManagerAdapter Service serves as a bridge between DIVAnet and the Oracle DIVArchive Manager. It must be configured to provide remote access by other DIVAnet systems.

DIVAnet DbSync Service

The DIVAnet DbSync Service is responsible for synchronizing asset information from multiple DIVArchive sites, and storing the information in the DIVAnet database. DbSync communicates remotely with ManagerAdapter services on multiple sites to synchronize archived object information. DbSync is typically deployed along with the ClientAdapter. Both the DbSync service and ClientAdapter require direct access to the DIVAnet database.

DIVAnet User Interface (DIVAnetUI)

DIVAnetUI is a GUI application that allows the user to monitor DIVAnet requests, and view, copy, and delete DIVAnet assets (DIVA archived objects) across multiple

DIVArchive sites. All DIVAnet level requests can be monitored, whether issued through the API or through the UI itself. You can also view asset information for all configured DIVArchive sites, regardless of whether the asset was archived through DIVAnet. DIVAnetUI provides flexible ways of querying both request information and asset information.

General Security Principles

The following sections describe the fundamental principles that are required to use any application securely.

Keep Software up to Date

Stay current with the version of DIVAnet that you run. You can find current versions of the software for download at the Oracle Software Delivery Cloud:

`https://edelivery.oracle.com/`

Restrict Network Access to Critical Services

DIVAnet uses the following TCP/IP ports by default:

- `tcp/9801` is the default WebService port used by the DIVAnet ClientAdapter
- `tcp/7101` is the default API socket port used by DIVAnet ClientAdapter (you can configure other ports)
- `tcp/9800` is the default WebService port used by the DIVAnet ManagerAdapter

> **Note:** Not all of these ports must be exposed externally, and are based on configuration and usage.

Use Principle of Least Privilege where Possible

DIVAnet services should not be run as the `admin` or `root`. Running the services using a different operating system user (than the user used to administer the application) contributes to overall system security.

The DIVAnet Linux installer requires two users to complete DIVAnet installation - `diva` and an operating system user. Administrators and Operators use the `diva` account to install and monitor DIVAnet. The operating system user controls the DIVAnet services.

Firewalls must restrict ports to only those that are required. DIVAnet contains access control features (briefly described in Access Control) used to restrict users and systems to the least privilege possible.

Monitor System Activity

You must monitor system activity to determine how well DIVAnet is operating and whether it is logging any unusual activity. Check the log files located in the `$DIVANET_HOME/Program/log` folder.

Keep Up To Date on Latest Security Information

You can access several sources of security information and alerts for a large variety of software products at:

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

The primary way to keep up to date on security matters is to run the most current release of the DIVAnet software.

2

Secure Installation

This chapter outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

Understand Your Environment

To better understand security needs, the following questions must be asked:

Which resources need to be protected?

You can protect many of the resources in the production environment. Consider the type of resources to protect when determining the level of security to provide.

When using DIVAnet, you must protect the following resources:

DIVAnet Servers

DIVAnet is installed on a server attached to one or more disks (either a local or remote disk directly connected to the DIVAnet system). Independent access to these disks (not through DIVAnet) presents a security risk. This type of external access might be from a rogue system that reads or writes to these disks, or from an internal system that accidentally provides access to these disk devices.

Database

There are database software and data resources used to build DIVAnet systems. The data exists typically on local or remote disks connected to the DIVAnet systems. Independent access to these disks (not through DIVAnet) presents a security risk. This type of external access might be from a rogue system that reads or writes to these disks, or from an internal system that accidentally provides access to these disk devices.

DIVArchive Sources, Destinations, and Archive Media

DIVAnet uses DIVArchive Sources and Destinations, and DIVA archival systems (disk or tape) in the process of satisfying its requests. Unwarranted independent access to these server disks and system medium, which are typically controlled by DIVArchive systems, is a security risk. The Source/Destinations that are used as temporary data stores for DIVAnet copy operations, should have restricted access, and you should consider dedicating these Source/Destinations solely to DIVAnet operations - and also ensure that the transfers are encrypted or initiated over a trusted network.

Configuration Files and Settings

DIVAnet system configuration settings must be protected from operating system level non-administrator users. In general, these settings are protected automatically by operating system level administrative users. Making the configuration files writable to non-administrative operating system users presents a security risk.

From whom are the resources being protected?

In general, the resources described in the previous section must be protected from all non-administrator access on a configured system, or from rogue external systems that can access these resources through the WAN or FC fabric.

What will happen if the protections on strategic resources fail?

Protection failures against strategic resources can range from inappropriate access (that is, access to data outside of normal DIVAdirector operations) to data corruption (erroneously deleting assets, or writing to disk or tape outside of normal permissions).

Recommended Deployment Technologies

This section describes installation and configuration of a secure infrastructure component.

For information about installing DIVAnet, refer to the *Oracle DIVAnet Installation, Configuration, and Operations Guide* in the *DIVAnet 2.1 Documentation* library at:

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

Consider the following points when installing and configuring DIVAnet.

DIVAnet Installation

You should install only those DIVAnet components that you require. For example, if you plan to run only DIVAnetUI from a client computer, deselect the **DIVAnet Services** in the list of components to be installed during installation. The default DIVAnet installation directory permissions and owners should not be changed after installation without considering the security implications of such changes.

Connecting to DIVArchive

Oracle recommends that you install the ManagerAdapter component on the DIVArchive Manager system for increased system security. If external access to the DIVArchive Manager port is not needed, it is recommended to block the port using firewall software. In addition, it will often not be necessary to allow external network access to the DIVAnet DbSync WebService port.

If you connect to a remote DIVArchive instance over a WAN, ensure that you connect over a trusted network. Also, consider connecting to the site using `SSL/TLS` to the remote site's ManagerAdapter port.

Safeguard Disk Systems

Use FC Zoning to deny access to the DIVAnet disks connected through Fibre Channel from any server that does not require access to the disks. Preferably, use a separate FC switch to physically connect only to the servers requiring access.

SAN RAID disks can usually be accessed for administrative purposes through TCP/IP or more typically HTTP. You must protect the disks from external access by limiting the administrative access to SAN RAID disks to systems only within a trusted domain. Also, change the default password on the disk arrays.

Postinstallation Configuration

After installing any portion of DIVAnet, go through the Security Checklist in Appendix A.

3

Security Features

To avoid potential security threats, customers operating DIVAnet must be concerned about authentication and authorization of the system.

These security threats can be minimized by proper configuration and by following the postinstallation checklist in Appendix A.

The Security Model

The critical security features that provide protections against security threats are:

- **Authentication -** Ensures that only authorized individuals are granted access to the system and data.
- **Authorization -** Access control to system privileges and data. This feature builds on authentication to ensure that individuals get only appropriate access.

Authentication

DIVAnet services can perform authentication using several methods:

- **SSL / TLS Certificates** - DIVAnet consults a certificate truststore when DIVAnet creates an outbound connection to a remote DIVAnet service. This helps to insure that DIVAnet is connecting to genuine DIVAnet services. To create a secure connection from the DIVAnet ClientAdapter to a DIVArchive instance, you must connect through the ManagerAdapter using a `ConnectionType` identified as **WebServices**.
- **Access Rules** - While technically a form of access control, access rules can filter inbound connections based on the inbound IP address. This feature is necessary to help insure that only approved systems have appropriate access to DIVAnet services.

> **WARNING: DIVAnet services use database passwords as part of their configuration. Passwords must be changed immediately after installation and every 180 days (minimum) thereafter. After the change has been made, you must store the passwords in a safe location, offline, where they can be made available for Oracle Support if needed.**

Access Control

Access rules can be created to limit the operations that certain users or systems may perform in the distributed archive system. Access rules can be run in the following ways:

- **ClientAdapter /MultiDiva Mode** - Restricts the types of DIVAnet requests that can be executed.
- **ManagerAdapter** - Restricts the types of DIVArchive requests that can be executed to satisfy a DIVAnet request (possibly requested by a remote system).

Access rules can affect requests initiated from the DIVAnetUI or from an API socket connection (possibly initiated by a MAM or automation system).

A DIVAnet request can have access rules executed on it at the DIVAnet level or at the DIVArchive level. At the DIVAnet level, the ClientAdapter processes the request where the request was received. At the DIVArchive level, a remote ManagerAdapter processes DIVArchive requests issued to satisfy the DIVAnet request.

Oracle recommends you create the most restrictive set of rules that meet your application requirements. For example, if only administrators need to perform global deletes, insure that others are denied access to that functionality. If a group of system users only require access to a finite list of Sources and Destinations, insure that those users can issue requests against only those specific Sources and Destinations.

Also consider the sites used to satisfy requests. For example, if users on the local site have no reason to perform copies where neither the source nor target sites are the local site (this is possible using DIVAnet), configure these rules in the ClientAdapter configuration.

Finally, consider specific constructs in requests you want to exclude across the board. For example, if you do not need to address objects with only the Object Name (without the category), then exclude all requests having blank categories.

Additionally, each ClientAdapter WorkflowProfile contains the list of valid messages that can be processed by requests assigned to the WorkflowProfile. In **MultiDiva Mode**, this provides a way of excluding a specific messages from processing (including informational messages).

Oracle recommends starting with the default rules defined in the `AccessRules.xml.ini` file even if you do not define your own access rules. For more information on DIVAnet Access Control features, refer to the *Oracle DIVAnet Installation, Configuration, and Operations Guide* at:

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

Configuring SSL/TLS

DIVAnet contains certificate data in two places: a *private keystore*, used for web services hosted on the local system, and a *public keystore*, used to verify web services that are invoked remotely. You can use the Java Keytool Utility to change the keystore password and add and delete certificates.

Refer to the following for more information regarding creating keystores:

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

Only the DIVAnet web services connections use SSL/TLS. In this release, connecting to DIVArchive or DIVAnet using a DIVArchive API socket connection will not use SSL/TLS.

Private Keystore

DIVAnet private key certificate data is stored in:

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

Exactly one certificate must appear in this keystore. This certificate is used for web services hosted by services running from this `$DIVANET_HOME` directory. It is recommended to replace the shipped certificate with a new certificate, and use a different certificate for each DIVAnet site in your network.

You must change the password of this keystore. Store the password information in a new file named `$DIVANET_HOME/Program/divanet/lib/diva129.properties`, and make this file readable by DIVAnet services (in Linux this user is `divanetsvc`), but not readable by casual users of the system (for example, the `diva` user in Linux). Use the following format for the file:

`keystorePassword=`*`newpassword`*

Public Keystore

Sometimes referred to as the *truststore*, this data is located in:

`$DIVANET_HOME/Java/lib/security/cacerts2`

This certificate data is used in outbound web service calls (including DIVAnetUI). Multiple public keys can be loaded into this keystore.

If you added a new self-signed certificate into the DIVAnet private keystore, export the certificate using the keytool utility. All of the applications (DIVAnet services, DIVAnetUI, and so on) that invoke WebServices on this site should then add the exported certificate to their own public keystore.

A

Secure Deployment Checklist

1. Set strong passwords for the Administrator and any other operating system accounts that have any DIVAnet administrator or service roles assigned to them. This includes:
   - `diva`, `divanetsvc`, and Oracle User IDs if being used
   - Any disk administrative accounts
2. Do not use a local administrator operating system account, instead assign roles as needed to other user accounts.
3. Use site-specific certificates for each DIVAnet installation, and define a strong password for the Oracle database and private keystore. Set a strong password for the Oracle database operating system login.
4. Install firewall software on every DIVAnet system and apply the default DIVAnet port rules. Restrict access to the DIVAnet API socket (`tcp 7101`) to IPs that require access using firewall rules. Perform this step with DIVAnet's Access Rules.
5. Install operating system and DIVAnet updates on a periodic basis since they include security patches.
6. Install antivirus and exclude the DIVAdirector processes and storage for performance reasons.
7. Best practices dictate segregation of FC disks and FC tape drives either physically or through FC Zoning so that disks and tape devices do not share the same HBA port. This security practice helps prevent loss-of-data accidents resulting from accidental overwriting important data.
8. Configure an appropriate set of backups for the DIVAnet configuration and database. Backups are part of security and provide a way of restoring data lost either accidentally, or through some breach. Your backup should include some policy while being transported to an off-site location. Backups need to be protected to the same degree as DIVAnet disks.