Oracle® Audit Vault and Database Firewall

Installation Guide

Release 20
E93405-34
February 2025

Oracle Audit Vault and Database Firewall Installation Guide, Release 20

E93405-34

Contents

B Installing Oracle AVDF on Oracle Database Appliance (ODA)

Preface

This section contains the following:

Audience

Oracle Audit Vault and Database Firewall Installation Guide is intended for anyone who is responsible for installing Oracle AVDF.

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

See Oracle Audit Vault and Database Firewall Release 20 Books.

Conventions

This document uses these text conventions:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Translation

This topic contains translation (or localization) information for Oracle AVDF User Interface and Documentation.

The Web based User Interface or the Audit Vault Server console is translated and made available in the following languages. This includes the User Interface, error messages, and help text.

- French
- German
- Italian
- Japanese
- Korean
- Spanish
- Portuguese - Brazil
- Chinese - Traditional
- Chinese - Simplified

Oracle AVDF Documentation is available in the following languages:

- English
- Japanese

Changes in Oracle AVDF

Learn about what's new when installing or updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

Changes in Oracle Audit Vault and Database Firewall Release 20

To learn what's new in the latest release of Oracle AVDF, 20.12, see the Oracle AVDF Release Notes guide.

1

Overview of Oracle Audit Vault and Database Firewall Installation

Learn to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide* for general information about secure installation, data protection, and general recommendations for deploying Oracle Audit Vault and Database Firewall in a network and in special configurations.

1.1 Learning About Oracle Audit Vault and Database Firewall

Learn more about Oracle Audit Vault and Database Firewall (Oracle AVDF).

Monitoring database activity to support incident investigation, detect potentially malicious behavior, and fulfill regulatory requirements is essential. Enabling either database auditing or monitoring network events can help you to get this visibility.

Database Activity Monitoring (DAM) is a security technology for monitoring and analyzing database activity. DAM solutions are used to identify and report on fraudulent, illegal, or other undesirable behavior and typically used to address security and compliance needs.

Oracle Audit Vault and Database Firewall (Oracle AVDF) supports native database audit data collection and network-based SQL monitoring to deliver a comprehensive Database Activity Monitoring solution.

Activity monitoring is essential, but organizations are also worried about the security posture of their databases. Were best practices followed when configuring the databases? Are databases in compliance with security standards? What else should be considered to strengthen the Oracle Database further? Database security posture management (DSPM) helps answer those questions, combining the ability to assess database configuration and security settings with sensitive data discovery to provide an integrated picture of a database's risk and security posture.

Oracle AVDF 20.9 and later expands the product's capabilities from database activity monitoring (DAM) to database security posture management (DSPM).

Oracle AVDF expands beyond database activity monitoring to manage your Oracle Database's security posture. AVDF's best-in-class activity monitoring capabilities are enhanced with visibility into security configuration, user entitlements, stored procedures, and how much and what types of data are in the database.

See the*Oracle Audit Vault and Database Firewall Concepts Guide* for more information about the features, components, users, and deployment of Oracle Audit Vault and Database Firewall.

1.2 Platform Support

Learn about various platforms supported by Oracle AVDF.

1.2.1 Product Compatibility Matrix

See which platforms are supported for installing Oracle Audit Vault and Database Firewall (Oracle AVDF), audit collection, database firewall support, and deploying the Audit Vault Agent and Host Monitor Agent.

Summary of Supported Platforms:

- Supported Hardware
- Supported Virtualization Platforms
- Audit Collection and Database Firewall Support for Databases
- Audit Collection Support for Operating Systems
- Audit Collection Support for Directory Services
- Audit Collection Support for File Systems
- Supported Operating Systems for Audit Vault Agent and Host Monitor Agent
- Support for Transaction Log Audit Collection Using Oracle GoldenGate

> **Note:**
>
> Oracle recommends that you update to the latest supported releases or versions at all times to stay current with security and functionality. Interoperability and functionality with older versions of the targets increases complexity and vulnerability.

> **Tip:**
>
> See Behavior Changes, Deprecated, and Desupported Platforms and Features to see the latest deprecation and desupport notices.

1.2.1.1 Supported Hardware

Oracle Audit Vault and Database Firewall (Oracle AVDF) is delivered as software appliance images that are ready to deploy on physical hardware or in virtualized environments, such as Oracle VM Server or VMware.

You can install and run Oracle AVDF on any Intel x86 64-bit hardware platform that is supported by Oracle AVDF's embedded operating system. Oracle AVDF release 20 uses the following Oracle Linux releases:

Oracle AVDF Release Update	Supported Oracle Linux release
Oracle AVDF 20.1 to 20.5	Oracle Linux version 7.8 with Unbreakable Enterprise Kernel (UEK) release 5

Oracle AVDF Release Update	Supported Oracle Linux release
Oracle AVDF 20.6 to 20.8	Oracle Linux release 7.9 with UEK release 6
Oracle AVDF 20.9 and later	Oracle Linux release 8.5 with UEK release 6

To determine whether your hardware is certified for Oracle Linux, see Hardware Certification List for Oracle Linux and Oracle VM. All Oracle Linux 7 and Oracle Linux 8 updates are also certified, unless otherwise noted.

> **Note:**
>
> - Oracle AVDF 20 supports both BIOS and UEFI boot mode. For systems with boot disks that are greater than 2 TB, Oracle AVDF supports booting in UEFI mode only.
> - Oracle AVDF can't be installed on Oracle Exalogic or Exadata appliances.

Related Topics

- Oracle Linux Documentation
- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

1.2.1.2 Supported Virtualization Platforms

Oracle Audit Vault and Database Firewall (Oracle AVDF) is delivered as software appliance images that are ready to deploy on physical hardware or in virtualized environments, such as Oracle VM Server or VMware.

- Oracle VM Server for x86, release 3.2.8, 3.2.9, 3.4.4, and 3.4.6
- VMWare VSphere, release 6.0, 6.7, and 7.0 (starting with Oracle AVDF 20.7)
- Oracle VM VirtualBox, release 5.2, 6.0, 6.1, and 7.0 (starting with Oracle AVDF 20.9)
- Kernel-based virtual machine (KVM)

The installation of Oracle AVDF on Amazon Web Services (AWS) is supported starting with Oracle AVDF 20.13. Installing AVDF on Amazon Web Services (AWS).

Prior to Oracle AVDF 20.13, the installation of Oracle AVDF on a non-Oracle Cloud platform (for example, AWS EC2) is not internally tested and supported by Oracle. You can conduct tests or proof of concept (POC) in your environment. You might be able to install Oracle AVDF on these platforms successfully. However, in case of any issue, Oracle Support will ask you to reproduce the issue on a supported platform of Oracle AVDF if the issue is already not known.

Related Topics

- Oracle Linux Documentation
- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

1.2.1.3 Audit Collection and Database Firewall Support for Databases

See which databases and versions are supported for audit collection and database firewall support in Oracle Audit Vault and Database Firewall (Oracle AVDF).

Supported Database	Versions Supported	Audit Collection Support	Database Firewall Support
Oracle Database (Enterprise and Standard editions)	21c (Starting with Oracle AVDF 20.4) 19c 18c 12.2 12.1 11.2.0.4	Yes	Yes
Oracle Autonomous Database Serverless (ADB-S, ATP-S, ADW-S)	Not applicable	Yes	Yes (Starting with Oracle AVDF 20.8)
Oracle Autonomous Database on Dedicated Exadata Infrastructure (ADB-D, ATP-D, ADW-D)	Not applicable	Yes (Starting with Oracle AVDF 20.3)	Yes (Starting with Oracle AVDF 20.8)
Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D)	Not applicable	Yes	Yes (Starting with Oracle AVDF 20.8)
Oracle Base Database Service	23ai (Starting with Oracle AVDF 20.13) 21c (Starting with Oracle AVDF 20.4) 19c	Yes	Yes (Starting with Oracle AVDF 20.8)
Oracle Database running on Exadata	23ai (Starting with Oracle AVDF 20.13) 21c (Starting with Oracle AVDF 20.4) 19c 18c 12.2 12.1 11.2.0.4	Yes	Yes
Oracle Real Application Clusters (Oracle RAC)	21c (Starting with Oracle AVDF 20.4) 19c 18c 12.2 12.1 11.2.0.4	Yes	Yes
MySQL (Enterprise Edition)	8.0 5.7 5.6	Yes	Yes

Supported Database	Versions Supported	Audit Collection Support	Database Firewall Support
Microsoft SQL Server (Windows) Enterprise Edition Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.	2022 (Starting with Oracle AVDF 20.10) 2019 (Starting with Oracle AVDF 20.3) 2017 2016 2014 2012	Yes	Yes
Microsoft SQL Server (Windows) Standard Edition	2022 (Starting with Oracle AVDF 20.10) 2019 (Starting with Oracle AVDF 20.6)	Yes	Yes (Starting with Oracle AVDF 20.8 support for Microsoft SQL Server Standard Edition 2019)
Microsoft SQL Server Cluster (Windows Failover Cluster) Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.	2019 (Starting with Oracle AVDF 20.6) 2017 2016 2014 2012	Yes	Yes (Starting with Oracle AVDF 20.6 support for Microsoft SQL Server Cluster 2019)
Microsoft SQL Server Always On availability group (Starting with Oracle AVDF 20.3) Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.	2017 2016 2014 2012	Yes	Yes (Starting with Oracle AVDF 20.11)
MongoDB (By configuring Quick JSON collector)	5.0 (Starting with Oracle AVDF 20.8) 4.4 (Starting with Oracle AVDF 20.4) 4.2 4.0	Yes	No
PostgreSQL (Open source only)	15 (Starting with Oracle AVDF 20.10) 14 (Starting with Oracle AVDF 20.10) 13 (Starting with Oracle AVDF 20.8) 12 (Starting with Oracle AVDF 20.8) 9.6 to 11.8	Yes	No
IBM Db2	11.5 11.1 10.5	Yes	Yes
IBM Db2 Cluster HADR (High Availability and Disaster Recovery) on OL 7.x	11.1	Yes	Yes

Supported Database	Versions Supported	Audit Collection Support	Database Firewall Support
IBM Db2 for AIX 7.2 TL1 and above 7.1 TL4 and TL5	11.5 11.1 10.5	Yes	Yes (Starting with Oracle AVDF 20.4)
IBM DB2 Database Partitioning Feature (DPF) on Linux and AIX	11.5 11.1 10.5	Yes	No
SAP Sybase ASE	16 15.7	Yes	Yes

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

1.2.1.4 Audit Collection Support for Operating Systems

See which operating systems(OS) and versions are supported for audit collection in Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **Note:**
>
> Audit log monitoring for the OS is supported through audit collection and not from the Database Firewall.

Supported Operating System	Versions Supported	Audit Collection Support
Oracle Solaris (SPARC64)	11.3 11.4	Yes
Oracle Solaris (x86-64) Solaris - x86-64 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.	11.3 11.4	Yes

Supported Operating System	Versions Supported	Audit Collection Support
Oracle Linux (64 bit)	OL 9 (requires auditd 3.0.7) (Oracle AVDF 20.9 and later) OL 8.2 and 8.3 (requires auditd 3.0) (Oracle AVDF 20.4 and later) OL 8 (requires auditd 3.0) (Oracle AVDF 20.3 and later) OL 7.9 (requires auditd 2.8) (Oracle AVDF 20.4 and later) OL 7.6-7.8 (requires auditd 2.8) (Oracle AVDF 20.2 and later) OL 7.4-7.5 (requires auditd 2.7.6) OL 7.3 (requires auditd 2.6.5) OL 7.1-7.2 (requires auditd 2.4.1) OL 7.0 (requires auditd 2.3.3) OL 6.8-6.9 (requires auditd 2.4.5) OL 6.6-6.7 (requires auditd 2.3.7) OL 6.1-6.5 (requires auditd 2.2.2) OL 6.0 (requires auditd 2.0)	Yes
Red Hat Enterprise Linux	RHEL 9 (requires auditd 3.0.7) (Oracle AVDF 20.9 and later) RHEL 8.2 and 8.3 (requires auditd 3.0) (Oracle AVDF 20.4 and later) RHEL 8 (requires auditd 3.0) (Oracle AVDF 20.3 and later) RHEL 7.9 (requires auditd 2.8) (Oracle AVDF 20.4 and later) RHEL 7.6-7.8 (requires auditd 2.8) (Oracle AVDF 20.2 and later) RHEL 7.5 (requires auditd 2.7.6) RHEL 7.4 (requires auditd 2.7.6) RHEL 7.3 (requires auditd 2.6.5) RHEL 7.2 (requires auditd 2.4.1) RHEL 7.1 (requires auditd 2.4.1) RHEL 7.0 (requires auditd 2.3.3) RHEL 6.10 (requires auditd 2.4.5) RHEL 6.9 (requires auditd 2.4.5) RHEL 6.8 (requires auditd 2.4.5) RHEL 6.7 (requires auditd 2.3.7)	Yes
Microsoft Windows Server (x86-64) Microsoft Windows 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.	2019 (Oracle AVDF 20.2 and later) 2016 2012 R2 2012	Yes
IBM AIX on Power Systems (64-bit)	7.3 (TL0) (Oracle AVDF 20.10 and later) 7.2 (TL2 and above) 7.1 (TL5)	Yes

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

1.2.1.5 Audit Collection Support for Directory Services

See which directory services and versions are supported for audit collection support in Oracle Audit Vault and Database Firewall (Oracle AVDF).

Supported Directory Service	Versions Supported	Audit Collection Support
Microsoft Active Directory	2012 to 2016	Yes

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

1.2.1.6 Audit Collection Support for File Systems

See which file systems and versions are supported for audit collection support in Oracle Audit Vault and Database Firewall (Oracle AVDF).

Supported File System	Versions Supported	Audit Collection Support
Oracle ACFS	12c	Yes

> **Note:**
>
> Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and desupported in 20.8.

Related Topics

- Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.7

1.2.1.7 Supported Operating Systems for Audit Vault Agent and Host Monitor Agent

See which operating systems and versions are supported for deploying the Audit Vault Agent and Host Monitor Agent.

Table 1-1 Oracle Linux (64 bit) Supported Versions

Versions Supported	Oracle AVDF Version	auditd Version Required	Audit Vault Agent Deployment	Host Monitor Agent Deployment
OL 9.x	20.9 and later	auditd 3.0.7	Yes	Yes

Table 1-1 (Cont.) Oracle Linux (64 bit) Supported Versions

Versions Supported	Oracle AVDF Version	auditd Version Required	Audit Vault Agent Deployment	Host Monitor Agent Deployment
OL 8.x All minor version of Oracle Linux 8 are supported, but only the listed versions have been certified and tested. Contact Oracle Support for help with non-certified versions of OL 8.	20.3 and later • OL 8.9 certified on 20.11 and later • OL 8.2 and 8.3 certified on 20.4 and later	auditd 3.0	Yes	Yes
OL 7.9	20.4 and later	auditd 2.8	Yes	Yes
OL 7.6-7.8	20.2 and later	auditd 2.8	Yes	Yes
OL 7.4-7.5	20.x	auditd 2.7.6	Yes	Yes
OL 7.3	20.x	auditd 2.6.5	Yes	Yes
OL 7.1-7.2	20.x	auditd 2.4.1	Yes	Yes
OL 7.0	20.x	auditd 2.3.3	Yes	Yes
OL 6.8-6.9 Oracle Linux 6 was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases.	20.x	auditd 2.4.5	Yes	Yes
OL 6.6-6.7 Oracle Linux 6 was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases.	20.x	auditd 2.3.7	Yes	Yes
OL 6.1-6.5 Oracle Linux 6 was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases.	20.x	auditd 2.2.2	Yes	Yes
OL 6.0 Oracle Linux 6 was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases.	20.x	auditd 2.0	Yes	Yes

Table 1-2 Oracle Linux (64 bit) Cluster Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
OL 7.x	20.x	Yes	No

Table 1-3 Red Hat Linux (64 bit) Supported Versions

Versions Supported	Oracle AVDF Version	auditd Version Required	Audit Vault Agent Deployment	Host Monitor Agent Deployment
RHEL 9.x	20.9 and later	auditd 3.0.7	Yes	Yes
RHEL 8.x All minor version of Red Hat Enterprise Linux 8 are supported, but only the listed versions have been certified and tested. Contact Oracle Support for help with non-certified versions of RHEL 8.	20.3 and later • RHEL 8.8 and 8.9 certified on 20.11 and later • RHEL 8.2 and 8.3 certified on 20.4 and later	auditd 3.0	Yes	Yes
RHEL 8.9	20.11 and later	Not applicable	Yes	Yes
RHEL 8.8	20.11 and later	Not applicable	Yes	Yes
RHEL 8.3	20.4 and later	auditd 3.0	Yes	Yes
RHEL 8.2	20.4 and later	auditd 3.0	Yes	Yes
RHEL 7.9	20.4 and later	auditd 2.8	Yes	Yes
RHEL 7.6-7.8	20.2 and later	auditd 2.8	Yes	Yes
RHEL 7.4-7.5	20.x	auditd 2.7.6	Yes	Yes
RHEL 7.3	20.x	auditd 2.6.5	Yes	Yes
RHEL 7.1-7.2	20.x	auditd 2.4.1	Yes	Yes
RHEL 7.0	20.x	auditd 2.3.3	Yes	Yes
RHEL 6.8-6.10	20.x	auditd 2.4.5	Yes	Yes
RHEL 6.7	20.x	auditd 2.3.7	Yes	Yes

Table 1-4 Red Hat Enterprise Linux Cluster Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
RHEL 7.x	20.x	Yes	No

Table 1-5 Linux on IBM Z Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
Red Hat Enterprise Linux 9	20.10 and later	Yes	No
Red Hat Enterprise Linux 8	20.10 and later	Yes	No

Table 1-6 Linux for Arm Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
Oracle Linux 9	20.12 and later	Yes	No
Oracle Linux 8	20.12 and later	Yes	No
Oracle Linux 7	20.12 and later	Yes	No
Red Hat Enterprise Linux 9	20.12 and later	Yes	No
Red Hat Enterprise Linux 8	20.12 and later	Yes	No
Red Hat Enterprise Linux 7	20.12 and later	Yes	No

Table 1-7 Microsoft Windows Server (x86-64) Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
2022	20.12 and later	Yes	Yes
2019	20.2 and later	Yes	Yes
2016	20.x	Yes	Yes
2012 R2	20.x	Yes	Yes
2012	20.x	Yes	Yes

Table 1-8 IBM AIX on Power Systems (64 bit) Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
7.3 (TLS2)	20.13 and later	Yes	Yes
7.3 (TL0)	20.10 and later	Yes	Yes
7.2 (TL2 and above)	20.x	Yes	Yes
7.1 (TLS 5)	20.x	Yes	Yes

Table 1-9 IBM AIX on Power Systems (64 bit) Cluster Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
7.3 (TL0)	20.10 and later	Yes	No
7.2 (TL2 and above)	20.x	Yes	No
7.1 (TLS 5)	20.x	Yes	No

Table 1-10 Oracle Solaris (SPARC64) Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
11.4	20.x	Yes	Yes
11.3	20.x	Yes	Yes

Table 1-11 Oracle Solaris (x86-64) Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
11.4	20.x	Yes	Yes
11.3	20.x	Yes	Yes

Solaris - x86-64 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.

Table 1-12 HP-UX on Itanium Supported Versions

Versions Supported	Oracle AVDF Version	Audit Vault Agent Deployment	Host Monitor Agent Deployment
11.31	20.x	Yes	Not applicable

HP-UX on Itanium was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

1.2.1.8 Support for Transaction Log Audit Collection Using Oracle GoldenGate

See which versions of Oracle GoldenGate are supported for collecting transaction log audit data from supported database targets.

Minimum Supported Oracle GoldenGate Version	Supported Target Databases and Versions	Supported Oracle AVDF Release
Oracle GoldenGate 19c (19.1.0.0.4)	Oracle Database 11.2 to 19c	Oracle AVDF 20.1 to 20.9
Oracle GoldenGate 19c (19.1.0.0.200414)	Microsoft SQL Server 2012, 2014, 2016, 2017, 2019 Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.	Oracle AVDF 20.9
Oracle GoldenGate 21c (21.4)	Microsoft SQL Server 2017, 2019	Oracle AVDF 20.10 and later
Oracle GoldenGate 21c (21.9)	Oracle Database 19c	Oracle AVDF 20.10 and later
Oracle GoldenGate 21c (21.11)	MySQL 8.0	Oracle AVDF 20.11 and later

> **Note:**
>
> To support Oracle Databases before 12.2, Downstream Mining needs to be configured.

Related Topics

- Transaction Log Audit Data Collection for Oracle Database

- Transaction Log Audit Data Collection for Microsoft SQL Server
- Transaction Log Audit Data Collection for MySQL
- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

1.2.2 Supported Browsers

Learn what browsers are supported with Oracle Audit Vault and Database Firewall (Oracle AVDF).

Oracle Audit Vault and Database Firewall requires a JavaScript-enabled browser and supports the current and prior major release of Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Internet Explorer, and Microsoft Edge.

> **Note:**
>
> - Ensure that the browser version you are using supports TLS 1.2 protocol.
> - Microsoft Internet Explorer 11 is the prior major release, with Microsoft Edge being the current Microsoft browser. Support for Internet Explorer (IE) 11 is deprecated. Audit Vault Server console does not support Microsoft Internet Explorer 11 (and prior), starting with release 20.6.

Related Topics

- Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.6

1.2.3 Support for External Systems

Learn about external systems supported by Oracle Audit Vault and Database Firewall.

Starting in Oracle AVDF 20.12, Nmap versions 7.92 and 7.94 are supported for Database Discovery.

For the storage area network (SAN), iSCSI can be used to extend disk space for storing event data.

For archival, the following protocols are supported:

- Server message block (SMB)
- Secure copy protocol (SCP)
- Network file system (NFS)
  - NFS v3 only: Oracle AVDF 20.4 and later
    Starting in Oracle AVDF 20.9, NFS v3 over User Datagram Protocol (UDP) is not supported.
  - NFS v3 and v4: Oracle AVDF 20.1 and later
  - NFS v4 only: Oracle AVDF 20.1 and later
    In case you only have NFS v4 in your environment for archive or retrieve, then set the `_SHOWMOUNT_DISABLED` parameter to `TRUE` using the following steps:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Start SQL*Plus as `sqlplus /nolog` without the user name and password.
4. In SQL*Plus, run the following command:

   ```
   connect super administrator
   ```
5. Enter the password when prompted.
6. Run the following command:

   ```
   exec avsys.adm.add_config_param('_SHOWMOUNT_DISABLED','TRUE');
   ```

   You can check the current value of the `_SHOWMOUNT_DISABLED` parameter by running

   ```
   select avsys.adm.get_config_param('_SHOWMOUNT_DISABLED') from dual;
   ```

   You can reset the `_SHOWMOUNT_DISABLED` parameter by running

   ```
   exec avsys.adm.delete_config_param('_SHOWMOUNT_DISABLED');
   ```

If your NFS server supports and permits both v3 and v4 for archive or retrieve, then no action is required.

> **Note:**
>
> If you're using the OCI Marketplace image to provision the AVDF instance only NFS location is supported.

In addition, integration is offered with:

- Syslog
- E-mail

1.2.4 Audit Vault Agent: Supported and Tested Java Runtime Environment

Learn about the supported and tested Java Runtime Environment (JRE) for the Audit Vault Agent.

Table 1-13 lists supported versions of Java Runtime Environment (JRE).

Table 1-13 JRE Support Matrix

JRE Version	Release/Version
Oracle Java 1.8	1.8.0_45 and later
Oracle Java 11	11.0.3

Table 1-13 (Cont.) JRE Support Matrix

JRE Version	Release/Version
Oracle Java 17 (Starting with Oracle AVDF release 20.8)	17.0.2
Oracle Java 21 (Starting with Oracle AVDF release 20.12)	21.0.2

Note:

- JRE version 11 is not supported on AIX platform in Oracle AVDF release 20.7 and earlier. For AIX platform use JRE version 1.8.0_241 (minimum).
- JRE versions 11 and 17 are supported on AIX platform starting with Oracle AVDF release 20.8.

1.2.5 Compatibility with Oracle Enterprise Manager

Learn about the supported versions of Oracle Enterprise Manager and Oracle Audit Vault Database Firewall.

Oracle Audit Vault and Database Firewall (Oracle AVDF) plug-in provides an interface within Enterprise Manager Cloud Control for administrators to manage and monitor Oracle Audit Vault and Database Firewall components.

Table 1-14 lists supported versions of Oracle Enterprise Manager and Oracle Audit Vault Database Firewall.

Table 1-14 Oracle Enterprise Manager Support Matrix

Oracle Enterprise Manager Release	Oracle Audit Vault Database Firewall Release
24.1.0	20.10 and later
13.5.2	20.4 - 20.9
13.5.1	20.4
13.4	20.x
• 13.3 • 13.2.1	12.2.x

Note:

Oracle Audit Vault and Database Firewall (Oracle AVDF) plug-in is supported only with the above mentioned Enterprise Manager releases.

See Also:

- Refer to System Monitoring Plug-in User's Guide for Audit Vault and Database Firewall for complete information.
- Refer to MOS note (*Doc ID 2855345.1*) for more information to manually deploy Oracle Enterprise Manager 13.x Agent on Audit Vault Server using the pull method.

2

Oracle Audit Vault and Database Firewall Pre-Install Requirements

Learn about the requirements that your system must meet before you can install Oracle Audit Vault and Database Firewall (Oracle AVDF).

2.1 Oracle AVDF Deployment Checklist

Prerequisites or deployment checklist for installing Oracle Audit Vault and Database Firewall.

1. Ensure to meet the hardware requirements in sections Product Compatibility Matrix and Oracle Audit Vault and Database Firewall Hardware Requirements.
2. Review and follow the sizing requirements mentioned in My Oracle Support Doc ID 2092683.1 to ensure hardware has sufficient capacity. Review the sizing whenever there is increase in scale of targets.
3. Review, plan, and deploy High Availability in Oracle AVDF.
4. Check and resolve the Ensure That the Boot Partition Has at Least 500 MB.
5. Follow the guidelines in Audit Vault Agent Requirements.
6. Follow the guidelines in Host Monitor Agent Requirements.
7. Follow the guidelines in Audit Vault Server Post-Installation Tasks.
8. Follow the guidelines in Database Firewall Post-Installation Tasks.

2.2 Oracle Audit Vault and Database Firewall Hardware Requirements

Install each Audit Vault Server and each Database Firewall onto its own dedicated x86 64-bit server or virtual machine (VM).

> **Caution:**
>
> Don't install the Audit Vault Server or Database Firewall on a server or VM that is used for other activities, because the installation process formats the server, which deletes existing data and operating systems.

See Platform Support for all supported hardware and virtualization platforms.

2.2.1 Memory and Space Requirements

Learn about the minimum memory requirements for Oracle Audit Vault and Database Firewall.

Each x86 64-bit server must have the following minimum memory:

- Audit Vault Server: 8 GB[1]

> **Note:**
>
> – System memory reduction is not supported in Audit Vault Server after installation. However, you may increase system memory with no restrictions from AVDF as long as a reboot of AVDF is performed.
>
> – For Oracle AVDF 20.1, Audit Vault Server uses HugePages to manage memory for the embedded Oracle Database.

- Database Firewall: 8 GB

2.2.2 Disk Space Requirements

Learn about the minimum disk space requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Each x86 64-bit server must have a single local hard drive with a minimum of the following disk space:

- Audit Vault Server: 370 GB
- Database Firewall: 220 GB

> **Note:**
>
> - Oracle AVDF must be installed on the appliance's local disk storage. SAN storage is not supported as the default storage and boot device.
> - Any additional disks on Audit Vault Sever must be greater in size than the first disk.
> - Oracle Audit Vault and Database Firewall release 20 supports both BIOS and UEFI boot mode. For system with boot disk greater than 2 TB, Oracle AVDF supports booting in UEFI mode only.
> - Provisioning disks greater than 4PB each for fresh installation is not optimal. The disks equal to or under 4PB, ensure that only one disk partition is allocated per disk group on each physical disk.
> - For appliance hardware specification, refer to Oracle Audit Vault and Database Firewall Sizing Advice (My Oracle Support Doc ID 2092683.1).

File System Layout

The installer checks for a number of conditions before allowing the installation or upgrade to be completed. Memory allocation and space checks on specific directories is an important aspect.

A minimum of at least 8 GB of memory is required. You can force the upgrade process to complete if your system has a lower amount of memory (for example 4 GB). However it is not difficult to extend memory for Oracle Audit Vault and Database Firewall installation. Oracle Audit Vault and Database Firewall sends daily reminders to upgrade your system's memory.

[1] In this guide, 1 GB represents 2 to the 30th power bytes or in decimal notation 1,073,741,824 bytes.

The space checks mentioned here are a bare minimum, below which the upgrade is likely to fail.

File System	Space Check
/home	100 MB
/usr/local/dbfw	200 MB
/usr/local/dbfw/tmp	7.5 GB
/var/lib/oracle	31 GB for Audit Vault Server
/	2 GB
/tmp	1.4 GB
/var/dbfw	100 MB
/var/log	100 MB
/var/tmp	5 GB
/boot	1 GB

2.2.3 Network Interface Cards

Learn about the recommended number of network interface cards (NICs) for each x86 64-bit server.

Oracle recommends the following number of network interface cards (NICs) for each x86 64-bit server on which you install the following components:

Oracle AVDF does not support Niagara cards.

Table 2-1 Number of Network Interface Cards (NIC) Recommended for AVDF Appliances

AVDF Appliance	Minimum Number of NICs Recommended
Audit Vault Server	1
Database Firewall deployed in Monitoring (Out-of-Band) mode	2
Database Firewall deployed in Monitoring (Host Monitor) mode	2
Database Firewall deployed in Monitoring / Blocking (Proxy) mode without network separation.	1
Database Firewall deployed in Monitoring / Blocking (Proxy) mode with network separation.	3 1 NIC for management, 2 NICs for client and database network connections.

See Also:

Introduction to Oracle Database Firewall Deployment

2.2.4 Fiber Channel Based Multipath in Oracle AVDF

Learn about support for multipath in Oracle AVDF.

Oracle Audit Vault and Database Firewall 20.1 and later supports fiber channel based storage with multipath. The redundant paths in multipath can enhance performance and utilize features like dynamic load balancing, traffic shaping, automatic path management, and dynamic reconfiguration. The connection to the disk can be made through two fiber channel ports.

Here are some important aspects of multipath in Oracle AVDF:

- It is not supported with ISCSI storage.
- It does not support the device xvd*.
- Multipath is supported only for Audit Vault Server installation.
- Multipath is not supported for Database Firewall installation.
- It does not support removable block devices. Check for removable block devices in the system as they can lead to installation failure.

Note:

In case there are removable block devices in the system, the following error may be encountered during Audit Vault Server installation:

```
ERROR: Failed to check if the disk is in multipath
Traceback (most recent call last):
  File "/run/install/repo/partitions.py", line 386, in <module>
    main()
  File "/run/install/repo/partitions.py", line 372, in main
    write_partition_table( None )
  File "/run/install/repo/partitions.py", line 322, in write_partition_table
    part_table = generate_partition_table_data(dev_list)
  File "/run/install/repo/partitions.py", line 243, in
generate_partition_table_data
    raise RuntimeError("No disks detected")
RuntimeError: No disks detected
```

2.3 Oracle Audit Vault and Database Firewall Software Requirements

Learn about the software requirements for Oracle Audit Vault and Database Firewall.

2.3.1 Java SE Requirement

The `AVCLI` command line utility that the Audit Vault Server administrator uses and the `avpack` utility (which is part of the software development kit) require Java SE version 8 or 11.

Java 8 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features
  Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

2.3.2 Browser Requirements

Learn about the browser requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **Note:**
>
> See section Supported Browsers for more information on the supported browsers.

2.3.3 Target Requirements

For targets that are on Oracle Solaris running the LDoms Manager service, `svc:/ldoms/ldmd:default`, ensure that the target is using LDoms version 3.2.0.1 or later.

2.4 Installing Audit Vault Server on VMware

Important prerequisites for installing Audit Vault Server on VMware.

- You must set VMX configuration parameter *disk.EnableUUID* to `TRUE`. This must be done to enable proper mounting of disks. Without this setting, the Audit Vault Server installation on VMware will fail.
- You must set your virtual machine to use EFI boot. In some versions of VMware this is done by selecting the **VM Options** tab, then expanding **Boot Options**, and then choose `EFI` in the **Firmware** field. You must disable secure boot. Do not select the checkbox **Enable UEFI secure boot** field.

> **Note:**
>
> This EFI boot setting is required only for fresh installation of Audit Vault Server specifically when the disk size is more than 2TB. This setting is not required for upgrade.

2.5 Privileges Required to Install Oracle Audit Vault and Database Firewall

Learn about the privileges required to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

Any user can install Oracle Audit Vault and Database Firewall. You do not need administrative privileges to complete the installation.

2.6 Audit Vault Agent Requirements

Learn about the Audit Vault Agent requirements.

> **Note:**
>
> Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

Recommended Prerequisites for Installing Audit Vault Agent

1. Ensure that you meet the system requirements. See Product Compatibility Matrix.
2. Ensure that you meet the following Java requirements:
   - Install the supported Java version on the Audit Vault Agent. See Audit Vault Agent: Supported and Tested Java Runtime Environment.
   - Apply the latest Java patches.
   - Point the `JAVA_HOME` to the JRE/JDK directory and set the path before installing the Audit Vault Agent.
3. Ensure that the host machine on which the Audit Vault Agent is deployed has at least 512 MB RAM.
4. Apply the latest security patches for the OpenSSL libraries that are available from the OS vendor for the specific OS version on the host machine.
5. Ensure that the host machine on which the Audit Vault Agent is deployed has connectivity to the Audit Vault Server.

   In a high availability environment, it must have connectivity to both primary and standby Audit Vault Servers.
6. Ensure that two Audit Vault Server ports (1521 and 1522 by default) are configured for communication with the Audit Vault Agent.
7. If you use Network Address Translation (NAT) in the network between the Audit Vault Server and the host machine where the agent is deployed, then ensure that the IP address of the host machine is resolvable from the Audit Vault Server.
8. Ensure that the user has the required OS permissions to install the agent.

   For directory audit trails, the user must be able to access the audit trail location. See About Deploying the Audit Vault Agent for the OS permissions that are required for installing the agent.
9. Ensure that the Audit Vault Agent home directory is access protected.

   Only the *Agent* user should have write or execute permissions on the agent home directory.
10. Ensure that the Audit Vault Agent host machine system settings are access protected to prevent malicious users from making modification.
11. Ensure that the system time of the Audit Vault Agent and the target are synchronized.

    They can be in different time zones. The time difference between these two systems (considering time zone conversion) should not exceed two seconds.

Additional Requirements for Starting the Audit Vault Agent as a Service on Windows

For Oracle AVDF 20.4 and earlier releases, comply with one of the following prerequisites:

- Install the Visual C++ Redistributable for Visual Studio 2012 Update 4 package from Microsoft on the Windows host machine.

  Ensure that the `msvcr110.dll` file is available in the `C:\Windows\System32` directory.
- If the `msvcr110.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.

For Oracle AVDF 20.6 and later releases, comply with one of the following prerequisites:

- Install the Visual C++ Redistributable for Visual Studio 2017 package from Microsoft on the Windows host machine.

  Ensure that the `vcruntime140.dll` file is available in the `C:\Windows\System32` directory.
- If the `vcruntime140.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.

> **Note:**
>
> There is a known issue in Oracle AVDF 20.5 for starting Audit Vault Agent as a service on Windows. See Error When Starting Audit Vault Agent as a Service on Windows in Oracle AVDF 20.5 for complete information. This issue is resolved in Oracle AVDF 20.6 and later.

2.7 Host Monitor Agent Requirements

The Host Monitor Agent has different requirements for installation, depending on the platform.

To install the Host Monitor Agent on the Windows platform, follow these requirements:

- Ensure that the Audit Vault Agent is running on the database server machine.
- Follow the Npcap installation requirements for your Oracle Audit Vault and Database Firewall (Oracle AVDF) release.

  Host Monitoring on Windows requires Npcap for capturing network traffic.

  – For Oracle AVDF release 20.6 and later, Npcap is automatically installed along with the agent installation.

    Installing Npcap removes any existing installation of Npcap or WinPcap from the Windows host machine.

  – For Oracle AVDF release 20.5, Npcap is automatically downloaded along with the agent software (`agent.jar`) file.

    Use the Npcap installer file that is available under the `Agent_Home\hm` directory.

  – For Oracle AVDF release 20.4 and earlier, install Npcap from the `avdf20-utility.zip` bundle on Oracle Software Delivery Cloud. It is part of the Oracle AVDF installable files. Select the *WinPcap-API-compatible* option when installing Npcap.
- Install the latest version of the OpenSSL (1.1.1g or higher) libraries.

OpenSSL 1.1.1 and earlier on Windows platforms was deprecated in Oracle AVDF 20.11, and it will be desupported in one of the future releases. To prevent issues, you should move to OpenSSL 3.0.13 or later.

- Ensure that the Windows target machine has the latest update of the Visual C++ Redistributable for Visual Studio 2015 (`MSVCRT.dll (*)` or later) package from Microsoft installed.
- If a network firewall is present, allow communication on port range 2050 - 5200.

  This is required for communication between the database server and the Database Firewall.

To install the Host Monitor Agent on a Linux, Unix, AIX, or Solaris platform, follow these requirements:

- Ensure that the Audit Vault Agent is running on the database server machine.
- Ensure that the latest version of the following packages from the operating system vendor are installed for the specific operating system version on the database server machine:
  - Libcap (for Linux hosts only)
  - LibPcap
  - OpenSSL
- Ensure that `gmake` is installed for AIX database servers.

  For other Unix database server types (Linux, Unix, or Solaris), ensure that `make` is installed. This is required for the Host Monitor Agent to run successfully.
- If a network firewall is present, allow communication on port range 2050 - 5200.

  This is required for communication between the database server and the Database Firewall.
- Ensure that the input output completion ports (IOCP) setting is `available` for IBM AIX on Power Systems (64-bit).

  It's set to `defined` by default.
- Ensure that all directories in the path of the Host Monitor Agent install location have 755 as the permission bits, starting from the root directory.

  This is required because the Host Monitor Agent has to be installed in a *root*-owned location.
- Ensure that the Host Monitor Agent is installed by the *root* user.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

> **See Also:**
>
> Enabling and Using Host Monitoring for host monitoring instructions and prerequisites.

3

Downloading and Installing Oracle Audit Vault and Database Firewall

Learn how to download and install Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **See Also:**
>
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for important information about securing and protecting your data.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for instructions on deployment and activation of Audit Vault Agent.

3.1 About Oracle Audit Vault and Database Firewall Installation

Understand the process for installing Oracle Audit Vault and Database Firewall (Oracle AVDF).

Here are the steps for installing Oracle AVDF:

1. Understand the Oracle Audit Vault and Database Firewall components to be installed.
2. Plan the system configuration that best suits your needs.
3. Ensure that your system meets the pre-install requirements.
4. Complete the installation of Audit Vault Server.
5. Complete the installation of Database Firewall.
6. Complete the post-install configuration tasks.
7. Complete the registration of hosts and deployment of Agent.
8. Complete the registration of targets for audit collection and Database Firewall monitoring.

> **Note:**
>
> The Audit Vault Server and the Database Firewall server are software appliances. You must not make any changes to the Linux operating system through the command line on these servers unless following official Oracle documentation or under guidance from Oracle Support.

See Also:

- *Oracle Audit Vault and Database Firewall Concepts Guide* for information about the components.
- *Oracle Audit Vault and Database Firewall Administrator's Guide* to plan the system configuration that best suits your needs.
- Upgrading Oracle Audit Vault and Database Firewall from Release 12.2 to Release 20 for instructions to upgrade Oracle Audit Vault and Database Firewall from release 12.2 to release 20.
- Patching Oracle Audit Vault and Database Firewall Release 20 for instructions to update Oracle AVDF release 20 to the latest release update (RU).
- Oracle Audit Vault and Database Firewall Pre-Install Requirements
- Downloading and Installing Oracle Audit Vault and Database Firewall
- Post-Install Configuration Tasks
- Uninstalling Audit Vault Agents Deployed on Target Host Machines

3.2 Downloading and Verifying Oracle AVDF Software

Learn about downloading and verifying the software to install Oracle Audit Vault and Database Firewall.

For a fresh installation, you can download the Oracle Audit Vault and Database Firewall software from the Oracle Software Delivery Cloud. You cannot use this package to upgrade. To perform an upgrade from an existing deployment, you can download the upgrade software from the My Oracle Support website.

3.2.1 Downloading the Audit Vault and Database Firewall Software

For a fresh installation of Oracle Audit Vault and Database Firewall, you need to download the software from the Oracle Software Delivery Cloud

1. Use a web browser to access the Oracle Software Delivery Cloud portal: https://edelivery.oracle.com
2. Click **Sign In**, and if prompted, enter your **User ID** and **Password**.
3. In the **All Categories** menu, select **Release**. In the next field, enter **Oracle Audit Vault and Database Firewall**, and then click **Search**.
4. From the list that is displayed, select the **Oracle Audit Vault and Database Firewall** version you want to install. Or click the **Select** icon that appears against the specific release.
   The download is added to your cart. To check the cart contents, click **View Items** or **Continue** in the upper right of the screen.
5. In the next page, verify the details of the installation package, and then click **Continue**.
6. Read the **Oracle Standard Terms and Restrictions** displayed on the page. Select **I reviewed and accept the Oracle License Agreement** check box, and then click **Continue**.

The download page appears and displays the list of ISO files for *Oracle Audit Vault and Database Firewall*.

- Audit vault Server install:

Oracle AVDF 20.4 and later	Oracle AVDF 20.1 to 20.3
`Vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server **Note:** Starting with Oracle AVDF 20.4, there is a single Audit Vault Server ISO file and there is no need to concatenate.	Audit Vault Server installer file is split into 3 parts or files as follows: – `Vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server - Part 1 of 3 (MUST DOWNLOAD ALL THE 3 PARTS AND CONCATENATE BEFORE ATTEMPTING INSTALLATION) – `Vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server - Part 2 of 3 (MUST DOWNLOAD ALL THE 3 PARTS AND CONCATENATE BEFORE ATTEMPTING INSTALLATION) – `Vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server - Part 3 of 3 (MUST DOWNLOAD ALL THE 3 PARTS AND CONCATENATE BEFORE ATTEMPTING INSTALLATION) **Note:** Concatenate all the three ISO files to get Audit Vault Server 20.x ISO (`avdf-install.iso`) before proceeding with installation.

- Database Firewall install:
  `Vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Database Firewall

> **Note:**
>
> Verify the checksum value for both (the Audit Vault Server ISO file and the Database Firewall ISO file). In case of any error or mismatch in the checksum values, download the ISO files and validate the checksum values again.

- Database Firewall utility:
  `Vpart_number.zip` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Utilities. This bundle contains the following files:
  - Npcap installer required for Host Monitoring on Windows: `npcap-utility.zip`
  - Database Firewall utilities to examine Native Network Encryption traffic for Oracle Database and to gather session information from other database types: `dbfw-utility.zip`
  - `Utilities_README`: Instructions for deploying Npcap and Database Firewall utilities patch.
- Deprecated cipher utility bundle:

Oracle AVDF 20.4 and later	Oracle AVDF 20.1 to 20.3
Not applicable.	`Vpart_number.zip` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Deprecated-Cipher-Removal Utility **Note:** Apply the deprecated cipher removal patch on Audit Vault Server 20.x after installation. This is optional. However, it is highly recommended.

- `Vpart_number.pdf` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Release Notes

7. Next to the **Print** button, click **View Digest Details**.
   The listing for the ISO files expands to display the SHA-1 and SHA-256 checksum reference numbers for each ISO file.
8. Click **Download**. The **Download Manager Installation** screen is displayed. The size of the combined ISO files exceeds 11 GB, and takes time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.
9. Click **Download the installer**, and then click **Save File**.
10. Choose a location to save the ISO files. Click **Save**.
    Alternately, you can save each file individually by clicking its name and then specifying a location for the download.
11. (For Oracle AVDF 20.3 and earlier) Combine the three AVS ISO files into one ISO file.
    - Linux:

      ```
      # cat <part1 file name>.iso <part2 file name>.iso <part3 file name>.iso
      > avdf-install.iso
      ```

    - Microsoft Windows:

      ```
      copy /b <part1 file name>.iso+<part2 file name>.iso+<part3 file
      name>.iso avdf-install.iso
      ```

After you have successfully downloaded the Audit Vault and Database Firewall software, you will need to generate the checksum values.

3.2.2 Generating the Checksum Values

After downloading the Audit Vault and Database Firewall software, you need to generate the checksum values.

1. After the ISO files are downloaded to the specified location, generate a SHA256 checksum for the combined Audit Vault Server ISO file and the Database Firewall ISO file. For Oracle AVDF 20.4 and later, there is a single Audit Vault Server ISO file. For example, on a Linux machine run the following command to generate the checksum:

   ```
   $ sha256sum Vpart_number.iso
   ```

> **Note:**
>
> Ensure that the checksum matches the value specified in the Release Notes document that is available along with the installable files. In case of any error or mismatch in the checksum values, download the ISO files again, concatenate the Audit Vault Server ISO file (for Oracle AVDF 20.3 and earlier), and validate the checksum values again. For Oracle AVDF 20.4 and later, there is a single Audit Vault Server ISO file and there is no need to concatenate.

3.2.3 Copying the ISO Image to External Media

Optionally, the combined Audit Vault Server ISO image (or single Audit Vault Server image for Oracle AVDF 20.4 and later) or the DBFW ISO image can be copied to another media, like USB. If the files are copied to a Linux based USB medium, then execute these steps.

1. Execute the following command to open the Linux terminal:

   ```
   sudo su -
   ```

2. Execute the following command to discover the USB device:

   ```
   lsblk
   ```

3. Execute the following command to erase the data on the USB device:

   ```
   dd if=/dev/zero of=/dev/<USB device> status=progress conv=fdatasync
   ```

4. Execute the following command to copy the iso file directly to the USB device:

   ```
   dd if=avdf-install.iso of=/dev/<USB device> status=progress conv=fdatasync
   ```

5. Boot the system using the USB device. Ensure the appliance is configured to boot from the USB device.
6. If the files are copied to a Windows (EFI only - Extensible Firmware Interface) based USB medium, then execute these steps:
   a. Execute the following command to open the Windows command prompt and to load the *diskpart*:

      ```
      diskpart
      ```

   b. Execute the following command to discover the USB device:

      ```
      list disk
      ```

   c. Execute the following command to select the USB device:

      ```
      select disk 1
      ```

d. Execute the following commands to erase or format the data on the USB device:

```
clean


create partition primary


format fs=fat32 label=AVS_20_<x>_0_0_0
```

Or

```
format fs=fat32 label=DBFW_20_<x>_0_0_0
```

Where x is the specific RU release number in Oracle AVDF. For example, use `AVS_20_4_0_0_0` or `DBFW_20_4_0_0_0` for Oracle AVDF 20.4 (20 RU4).

e. Execute the following command to add Master Boot Record (MBR) to the USB device:

```
active
```

f. Execute the following command to exit the *diskpart*:

```
exit
```

3.3 Installing Audit Vault Server or Database Firewall

Steps for installing Audit Vault Server or Database Firewall.

Audit Vault Server and Database Firewall are delivered as software appliance images, ready to be deployed on physical machines or on virtual machines (VM). Start with the installation of Audit Vault Server and later install Database Firewall.

> **Note:**
>
> - For Oracle AVDF 20.4 and later, the Audit Vault Server ISO is a single file and there is no need to concatenate. You must combine the downloaded Audit Vault Server ISO files (for Oracle AVDF 20.3 and earlier) into a single ISO file, before starting the Audit Vault Server installation.
> - If you are installing Audit Vault Server on VMware, then set the VMX configuration parameter *disk.EnableUUID* to `TRUE`. Also, you must set your virtual machine to use EFI boot. In some versions of VMware this is done by selecting the **VM Options** tab, then expanding **Boot Options**, and then setting the firmware to EFI. You must disable secure boot.Without this setting, the Audit Vault Server installation on VMware will fail.

1. Choose the `.iso` file depending on whether you are installing on a Virtual Machine or a physical machine.

> **Note:**
>
> - In case the `.iso` file is available on the USB device, then ensure to boot the machine using the bootable USB disk created in the previous section to complete the installation.
> - In case the `.iso` file is available remotely on another host, then attach the `.iso` file using remote installation tools to complete the installation.

2. The system boots and the initial splash screen appears. It indicates the release number you are installing.
3. Press the **Enter** key. The installation proceeds.
4. Enter the new *root* password when prompted for change.
5. Enter the same password when prompted for confirmation.

   The system installs the operating system and then reboots.
6. Continue with the installation and sign in as *root* user on the console when prompted.

> **Caution:**
>
> Logging in as `root` during install or upgrade uses tmux, a terminal multiplexer, to display persistent information. A user with access to these screens can create new root shells. If you plan to leave the session unattended, Oracle recommends disconnecting from the blue screen by using the `CTRL-b d` command. To reconnect, log in as `root` once more.

7. The installation continues with the following prompts on the screen one after another:

```
Installing AVDF bootstrap
Beginning installation of Audit Vault Server dependencies
Creating repository.
Relinking Oracle Database
Installing AVS application.
OR
Installing Database Firewall.
Migrating repository to ASM storage
Updating Oracle Audit Vault and Database Firewall data
Updating UI

....
```

8. The installer prompts for network configuration. Select the appropriate network interfaces and click **OK**.
9. The following **Network settings** screen appears.

10. Enter the following fields:
    a. **IP Address** of the network interface
    b. **Network Mask**
    c. **Gateway**: Enter the IP address of the network interface if a gateway is required. Else, clear the field before saving.
11. Press **OK**.
12. Upon completion of the network settings, the installation continues.
13. Upon successful installation of Audit Vault Server, the following example (for Oracle AVDF 20.1) message is displayed:

```
Audit Vault Server 20.1.0.0.0 installation has completed.
Post install configuration steps must be completed using the
appliance administration console ...
```

14. Press **OK**. The installation of Audit Vault Server is complete.
15. Upon successful installation of Database Firewall, the following example (for Oracle AVDF 20.1) message is displayed:

```
Oracle Database Firewall 20.1.0.0.0 installation has completed.
```

16. The installer screen exits and automatically returns to the login prompt.

> **Note:**
>
> The Audit Vault Server and the Database Firewall server are software appliances. You must not make any changes to the Linux operating system through the command line on these servers unless following official Oracle AVDF documentation or under guidance from Oracle Support.

See Also:

- Post-Install Configuration Tasks
- In case of any installation failures encountered before or after reboot, use the solution mentioned in Collecting Logs To Debug Pre-reboot Installation Failure.

3.4 Installing AVDF on Amazon Web Services (AWS)

Starting with Oracle AVDF 20.13, the installation of AVDF on AWS is supported.

1. Install the AWS command line interface (CLI).
   See Installing or updating to the latest version of the AWS CLI and Setting up the AWS CLI from the AWS documentation for more information.
2. Create a S3 bucket.
   See Create your first S3 bucket from the AWS documentation for more information.
3. Create a `vmimport` user and assign it the necessary policies for import.
   See Required permissions for VM Import/Export from the AWS documentation for more information.
4. Upload the AVDF image to the S3 bucket.

   ```
   aws s3 cp your/path/to/image s3://your-bucket-name/image-name.vhd
   ```

   The AVDF image files, `avs.vhd` and `dbfw.vhd`, can be found from Oracle Software Delivery Cloud as part of the Audit Vault Server on AWS and Database Firewall on AWS downloads, respectively. You will have to unzip the provided files. See Downloading the Audit Vault and Database Firewall Software for more information.

   See the cp entry in the AWS CLI documentation for more information.
5. Create a `container.json` file containing the following:

   ```
   {
       "Description": "AVDF_AWS_216_IMAGE",
       "Format": "vhd",
       "UserBucket": {
           "S3Bucket": "avdf-images",
           "S3Key": "AVDF_AWS_216.vhd"
       }
   }
   ```

   Ensure that you change the name of the AVDF image file as necessary.
6. Create a snapshot from the image file in the S3 bucket. Use the `container.json` file created in the previous step.
   See Importing a disk as a snapshot using VM Import/Export from the AWS documentation for more information.
7. Create an Amazon Machine Image (AMI) using the snapshot.
   See Create an AMI from a snapshot from the AWS documentation for more information.

   For the **Virtualization type**, select **hardware virtual machine (HVM)**.

For the **Boot mode**, select **legacy-bios**.

8. Launch the instance from the AMI image.
   See Launch an EC2 instance using the launch instance wizard in the console from the AWS documentation for more information.

   Ensure the following:

   - Use, at minimum, an c5.xlarge with vCPU: 4 and Memory: 8Gb instance
   - For SSH key pairs, generate a `ed25519` key
   - If using a security group, allow imports from port 22 for SSH and ports 7443 and 443 for HTTP.

9. Perform the steps in Post Instance Creation Steps

   - Audit Vault Server:

     a. Log in to the appliance through SSH and switch to the `root` user.

        See Logging In to Oracle AVDF Appliances Through SSH.

     b. Change root user password by running the following command. The root password is required to troubleshoot the instance using OCI instance console connection.

        ```
        sudo passwd root
        ```

     c. Generate a one time passphrase by running the command:

        ```
        sudo -u oracle /usr/local/dbfw/bin/
        generate_post_install_passphrase.py
        ```

     d. Copy the passphrase that is returned by the above command.

     e. Access the Audit Vault Server console by entering `https://<IP address of the instance>` as the URL in the browser.

     f. Enter the passphrase copied from the earlier step in the **Post Install Authentication** page of the Audit Vault Server console.

     g. Fill in the details in the **Post Install Configuration** page.

     h. In the **AVS IP for Agent Communication** section, specify the public IP of the Audit Vault Server if you are expecting to collect audit data from any target outside of OCI. See section Deploying Audit Vault Agents for more details.

        > **Note:**
        >
        > After the post installation step is complete, changing the AVS IP for Agent communication is not supported.

     i. Click **Save**.
        DNS is automatically set to 169.254.169.254.

        > **See Also:**
        >
        > DNS in Your Virtual Cloud Network

   - Database Firewall:

a. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

b. Change root user password by running the following command. The root password is required to troubleshoot the instance using OCI instance console connection.

   ```
   sudo passwd root
   ```

10. SSH into the instance:

    a. Copy the downloaded `AWS_SSH.pem` file to `~/.ssh/` folder

       ```
       cp AWS_SSH.pem  ~/.ssh/
       ```

    b. Run the following command:

       ```
       ssh -i  "~/.ssh/AWS_SSH.pem" opc@<ip address>
       ```

Related Topics

- AWS VM Import/Export
- Launch an Amazon EC2 instance from an AWS Marketplace AMI

4
Post-Install Configuration Tasks

Learn about the post-installation tasks for Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **See Also:**
>
> Unable to Log in to the Oracle AVDF Appliance through SSH

4.1 Audit Vault Server Post-Installation Tasks

Complete these recommended post-installation tasks after installing the Audit Vault Server.

1. Complete the steps in section Accessing the Audit Vault Server Post-Install Configuration Page and set up user names and passwords.
2. Apply the patch to remove deprecated ciphers after an Audit Vault Server install or upgrade: `Deprecated-Cipher-Removal.zip`.

   > **Note:**
   >
   > Apply this patch on Oracle Audit Vault Server 20.1 after an install or upgrade. For an upgrade, before applying the patch, make sure that all Audit Vault Agents are upgraded to 20.1 and Host Monitor Agents are in the `Installed` state.

3. Review the DNS and NTP system service configuration. See Configuring or Changing the Oracle Audit Vault Server Services.
4. If using high availability, configure resilient pair of Audit Vault Servers. See Configuring High Availability for Audit Vault Servers.
5. Register the targets for monitoring with Oracle Audit Vault and Database Firewall. See Configuring Targets, Audit Trails, and Database Firewall Monitoring Points.
6. Configure the data retention policy for every target before configuring audit trails. See Configuring Archive Locations and Retention Policies.
7. Configure each audit trail for native audit collection. See Preparing Targets for Audit Data Collection.
   a. Deploy an Audit Vault Agent on the machine where the target is installed or on a machine that can connect to the target.

> **Note:**
>
> Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

b. Enable native database auditing on the target.

c. Review and configure the audit trails for the target.

d. Configure the audit trail cleanup wherever necessary.

8. For Oracle Database targets, consider provisioning Oracle recommended audit policies. See Creating Audit Policies for Oracle Databases.
   After patching to Oracle AVDF 20.12, you will need to

   a. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.

   b. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

9. Consider configuring alert policies. See Creating Alerts.

> **Note:**
>
> - The Audit Vault Server reads the audit log from the target that contains the time stamp of the event. Without this synchronization, events may appear to be archived to the Audit Vault Server before they occur and alerts may appear to be sent before their triggering events occur.
> - Set the user names and passwords of the Audit Vault Server administrator and auditor, as well as the passwords of its root and support users. You can also set the time and domain name service (DNS) servers of the Audit Vault Server.

4.2 Database Firewall Post-Installation Tasks

Learn about Database Firewall post-installation tasks.

After installing the Database Firewall, set the password for `support` user. This is the Linux operating system user account on Database Firewall. Follow these steps to set the password:

1. After the installation is complete, log in as `root` user on the console displayed.
2. Execute the following command to set the password for the `support` user:

   ```
   passwd support
   ```

3. Enter the new password for the `support` user when prompted.
4. Re-enter the password when prompted.
5. After the password is set successfully, the following message is displayed on the console:

```
all authentication tokens updated successfully.
```

4.3 Accessing the Audit Vault Server Post-Install Configuration Page

Access the Audit Vault Server post-installation configuration page.

To access the Audit Vault Server Post-Install Configuration page:

1. Using a browser, go to the Audit Vault Server console. Ensure that the browser version you are using supports TLS 1.2 protocol. See Supported Browsers for complete information.

   `https://ip_address`

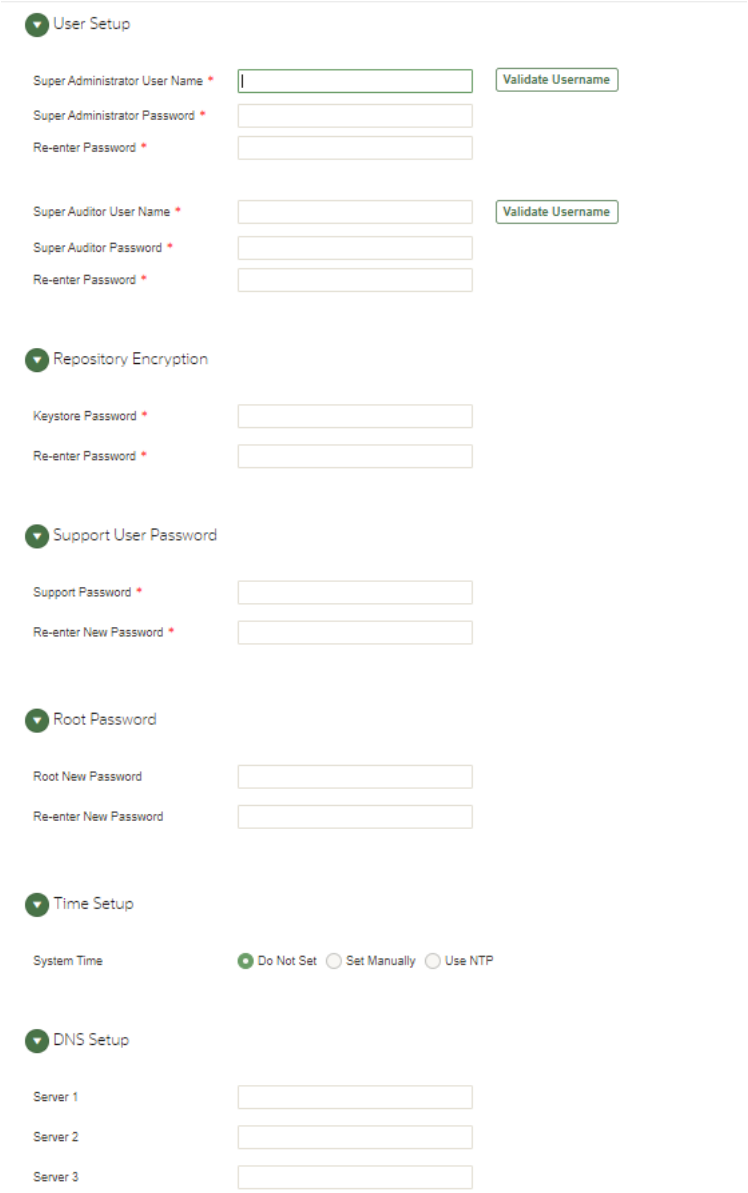
   For *ip_address*, use the IP address of the Audit Vault Server. See Installing Audit Vault Server or Database Firewall.

   You may see a message about a problem with the website security certificate. This is due to a self-signed certificate. Click the **Continue to this website** (or similar) link. You can generate a certificate request later to avoid this message. This is one of the possible reasons. However, there may be other reasons where the browser may prompt about the website being insecure. Use your due caution, verify, and then connect to the correct website.

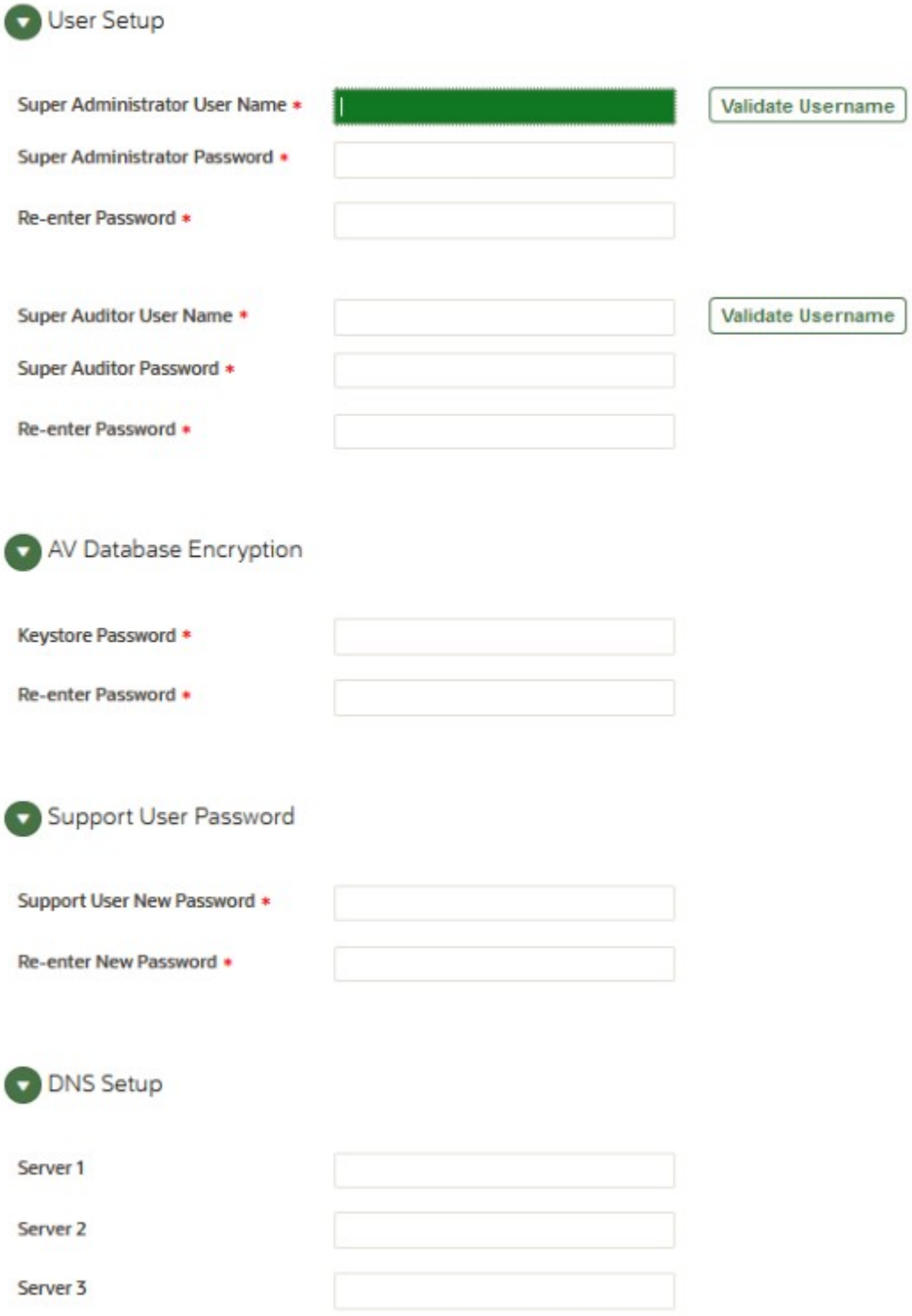
   See *Oracle Audit Vault and Database Firewall Administrator's Guide*.

2. You are prompted to enter the *root* password.
3. Click **Login**. The post-install configuration page appears.

   Post-Install Configuration page (Oracle AVDF release 20.1 to 20.7)



Post-Install Configuration page (Oracle AVDF release 20.8 and later):



4. From this page, you must set the usernames and passwords (required), set up the time, and DNS servers.

> **See Also:**
>
> Unable to Access the AVS Console After Changing the AVS Time Manually or using NTP Server

4.4 Setting the Usernames and Passwords of Audit Vault Server Users

Set up usernames and passwords for Oracle Audit Vault and Database Firewall (Oracle AVDF).

In the post-install configuration page, you set up usernames and passwords for the following *Oracle Audit Vault and Database Firewall* users:

- `Super Administrator`
- `Super Auditor`
- `Repository Encryption Keystore`
- `Support`
- `Root`

Changing the `root` user password on this screen is optional as it is already set during installation.

> **See Also:**
>
> Separation of Duties for a description of each user.

> **Note:**
>
> Do not use the root or support users unless instructed to do so in documentation or by a customer support representative.

4.4.1 About Administrator and Auditor User Names

Oracle recommends that you create administrator and auditor user accounts after you install Oracle Audit Vault and Database Firewall (Oracle AVDF).

The administrator and auditor user names must follow these rules:

- The first character has to be alphabetical.
- 1 to 30 characters long.
- Each remaining character is either alphanumeric or an underscore (_), dollar sign ($), or number sign (#).

> **Note:**
>
> The administrator and auditor user names are upshifted (that is, any lowercase alphabetic characters are replaced by their uppercase equivalents). Also, the Audit Vault Server does not support quoted user names.

> **See Also:**
>
> Separation of Duties for a description of each user account.

4.4.2 Password Requirements

Set password management guidelines for the Audit Vault and Database Firewall (Oracle AVDF) user accounts.

For example, you may require that users change their passwords on a regular basis, such as every 120 days, and that they create passwords that are not easily guessed.

The following sections describe the minimum password requirements for Oracle Audit Vault and Database Firewall.

Requirements for Passwords Containing Unicode Characters

If your password contains unicode characters (such as non-English characters with accent marks), the password requirement is that it:

- Be between 8 and 30 characters long.

Requirements for English-Only (ASCII) Passwords

If you are using English-only, ASCII printable characters, Oracle Audit Vault and Database Firewall requires that passwords:

- Be between 8 and 30 characters long.
- Contain at least one of each of the following:
  - Lowercase letters: a-z.
  - Uppercase letters: A-Z.
  - Digits: 0-9.
  - Punctuation marks: comma (,), period (.), plus sign (+), colon(:), exclamation mark (!), and underscore (_)
- Not contain double quotes ("), back space, or control characters.

In addition, Oracle recommends that passwords:

- Not be the same as the user name.
- Not be an Oracle reserved word.
- Not be an obvious word (such as welcome, account, database, and user).
- Not contain any repeating characters.

> **See Also:**
>
> - *Oracle Database Security Guide* for additional guidelines on how you can strengthen passwords for your site.
> - Changing Your Own Password
> - Changing the Password of Another Administrator

4.4.3 Setting the Passwords For Audit Vault Server Users

Steps for setting the passwords for the Audit Vault Server users.

To set the passwords of the Audit Vault Server administrator, auditor, root, and support user:

1. Access the Audit Vault Server Post-Install Configuration page.
2. Under **User Setup**:
   - In the **Super Administrator** field, enter the administrative user name.
   - Under the **Super Administrator** field, enter the administrator **Super Administrator Password**, then confirm it in the **Re-enter Password** field.
   - Click **Validate username**.

     The administrator username that you entered is validated. If this name is valid, then you can use it; if not, then you must enter a valid name.
   - In the **Super Auditor** field, enter the super auditor user name.
   - Under the **Super Auditor**, field, enter the auditor **Super Auditor Password**, then confirm it in the **Re-enter Password** field.
   - Click **Validate username**.

     The auditor username that you entered is validated. If this name is valid, then you can use it; if not, then you must enter a valid name.
3. Under **Repository Encryption**, enter the **Keystore Password**, and then re-enter it.

   On new, full installations of Oracle Audit Vault and Database Firewall 12.2 or later, audit event data in the Audit Vault Server's repository is automatically encrypted using Oracle Database Transparent Data Encryption (TDE). The repository encryption keystore password is required to reset the TDE master key.
4. Under **Root Password**, in the fields labeled **Root Password** and **Re-enter New Password**, type the password for root.
5. Under **Support User Password**, in the fields labeled **Support Password** and **Re-enter New Password**, type the password for the support user.

> **See Also:**
>
> Accessing the Audit Vault Server Post-Install Configuration Page

4.5 Setting the Audit Vault Server Time (Strongly Recommended)

Steps to set the Audit Vault Server time.

To set the Audit Vault Server time:

1. Access the Audit Vault Server Post-Install Configuration page.
2. Expand the **Time Setup** section.
3. Select either **Set Manually** or **Use NTP**.

> **Note:**
>
> Oracle strongly recommends that you select **Use NTP**. In addition, it is recommended that you also use an NTP service on your targets to avoid confusion on timestamps on the alerts raised by the Audit Vault Server.

4. If in step 3 you selected **Use NTP**, then for each of the fields **Server 1 Address**, **Server 2 Address**, and **Server 3 Address**:
   a. Type either the IP address or name of a preferred time server.

      If you type a name, the DNS server specified in the System Services page is used for name resolution.

   b. Click **Test Server**.

      The time from the specified server appears.
5. If in step 3 you selected **Set Manually**, then set the **Date** fields to your current local day and time.
6. Either click **Save** or proceed to set the DNS servers for the Audit Vault Server.

> **See Also:**
>
> Unable to Access the AVS Console After Changing the Audit Vault Server Time using NTP Server or Manually

4.6 Setting the Audit Vault Server DNS Servers (Recommended)

Steps to set the DNS servers for the Audit Vault Server.

The Audit Vault Server DNS servers are used to resolve any host names that Audit Vault Server might use.

> **Note:**
>
> Set Audit Vault Server DNS server values only if the network has DNS servers, otherwise system performance will be impaired.

To set the DNS servers for the Audit Vault Server:

1. Enter the IP addresses of up to three DNS servers on the network in the **Server 1**, **Server 2**, and **Server 3** fields.

   Leave the fields blank if there are no DNS servers.

2. Click **Save**.

4.7 Networking Setup And Configuration

Oracle Audit Vault and Database Firewall can be setup or configured for access through DNS.

The host name must match the FQDN used for access.

See Also:

- Changing Host Names
- *Oracle Audit Vault and Database Firewall Administrator's Guide*
- *Oracle Audit Vault and Database Firewall Administrator's Guide*
- Unable to Access the AVS Console After Changing the Audit Vault Server Time using NTP Server or Manually

5

Behavior Changes, Deprecated, and Desupported Platforms and Features

Review information about Oracle Audit Vault and Database Firewall changes, deprecations, and desupported features.

In addition to new features, Oracle Audit Vault and Database Firewall release updates can modify, deprecate, or desupport features and introduce upgrade behavior changes.

Be aware of the implications of deprecated and desupported.

- **Deprecated** features are no longer being enhanced but are still supported for the current release update (RU) of Oracle Audit Vault and Database Firewall. A deprecated feature can be desupported in the next release update of Oracle Audit Vault and Database Firewall.
- **Desupported** features are no longer supported by fixing bugs related to that feature. Often, Oracle can choose to remove the code required to use the feature.

5.1 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.13

- Traditional auditing is desupported in Oracle Database 23ai. Oracle recommends that you use unified auditing. However, if you upgrade an existing Oracle Database registered with Oracle AVDF to 23ai, any existing traditional audit policies will continue to work, but creating new or enabling previously disabled traditional audit policies is not allowed. For more information see Handling the Desupport of Traditional Auditing in the *Oracle Database Security Guide* and Traditional Auditing Desupported in the *Oracle Database Upgrade Guide*.

5.2 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.12

- Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.
- Microsoft Windows 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

5.3 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.11

- OpenSSL 1.1.1 and earlier on Windows platforms was deprecated in Oracle AVDF 20.11, and it will be desupported in one of the future releases. To prevent issues, you should move to OpenSSL 3.0.13 or later.

5.4 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.10

- Oracle Linux 6 was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases.

5.5 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.9

- Solaris - x86-64 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.
- HP-UX on Itanium was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.
- Java SE Requirement Java 8 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.

5.6 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.8

- Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was desupported in Oracle AVDF release 20.8
- Sybase SQL Anywhere was desupported in Oracle AVDF release 20.8

5.7 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.7

- Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7
- Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7

5.8 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.6

- Audit Vault Server console does not support Microsoft Internet Explorer 11 (and prior), starting with Oracle AVDF release 20.6.

5.9 Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.1

- The Database Firewall In-line Bridge deployment mode is desupported in Oracle AVDF release 20.1

- The Activity Overview Report captures information about all monitored and audited events is deprecated in Oracle AVDF release 20.1

6

Patching Oracle Audit Vault and Database Firewall Release 20

If you're on Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20, you can apply the most recent release update (RU) patch to access the latest features and bug fixes.

If you're on Oracle AVDF release 12.2, see Upgrading Oracle Audit Vault and Database Firewall from Release 12.2 to Release 20 to perform a full upgrade to release 20.

> **Note:**
>
> - The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.
> - This chapter uses the terms *update* and *patch* interchangeable.

6.1 About Patching Oracle Audit Vault and Database Firewall

Follow these guidelines for patching Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20 to the latest release update (RU).

Use the following high-level process to patch Oracle AVDF:

1. Download the files from My Oracle Support.
2. Complete the pre-update tasks, such as creating a backup.
3. Update the Audit Vault Servers.
4. Verify that Audit Vault Agents and Host Monitor Agents were updated automatically.
5. Update the Database Firewalls.
6. Complete the post-update tasks, such as confirming that the update was successful.

> **Note:**
>
> If you have a large amount of event data, maintain sufficient disk space of about 5% of the total event log data size. If you have both HDD and SAN storage, then maintain the necessary disk space on either HDD or SAN. Each disk group (EVENTDATA, SYSTEMDATA, and RECOVERY) should have at least 20% available space.

> **Note:**
>
> To updateOracle AVDF to a new release with minimal downtime for monitoring and collecting data, see Updating Oracle AVDF with Minimal Downtime by Using Backup and Restore.

6.2 Download the Files

To patch or upgrade Oracle Audit Vault and Database firewall (Oracle AVDF), you need to download files from My Oracle Support.

1. Go to My Oracle Support and sign in.
2. Click the **Patches & Updates** tab.
3. Use the **Patch Search** box to search for the patch.
   a. Click the **Product or Family (Advanced)** link on the left.
   b. In the **Product** field, enter *Audit Vault and Database Firewall*.
   c. In the **Release** field, select the latest Oracle AVDF release from the drop-down list.
   d. Click **Search**.
4. In the **Patch Name** column of the search results, click the link for the latest bundle patch.

6.3 Pre-update Tasks

Before updating Oracle Audit Vault and Database Firewall (Oracle AVDF) to the latest release, complete the prerequisite tasks, such as performing a backup.

> **Note:**
>
> If Audit Vault Agent is running on a Windows machine, close all the agent-related directories and open files before updating Oracle AVDF.

6.3.1 Back Up the Current Oracle Audit Vault and Database Firewall Installation

Before updating Oracle Audit Vault and Database Firewall (Oracle AVDF) to the latest release, back up the Audit Vault Server.

See Backing Up and Restoring the Audit Vault Server for complete information.

If your current Audit Vault Server is installed on a virtual machine (VM), such as Oracle VM or VMWare, Oracle recommends that you take a VM snapshot before starting the update process.

6.3.2 Release Existing Tablespaces That Are Retrieved Manually

If you're updating to Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.1 through 20.3, release all the existing tablespaces that were retrieved manually. This procedure is performed automatically if you're updating to Oracle AVDF release 20.4 or later.

The following steps are only applicable for AVDF 20.1 - 20.3.

If you don't release the existing tablespaces, the following situations could occur:

- The update might fail, resulting in an error.
- New indexes might not be created after the update because space can't be allocated.

To manually release the tablespaces, follow these steps:

1. Log in to the Audit Vault Server console as a *super administrator*.
2. Click the **Settings** tab.
3. Click **Archiving** in the left navigation menu.
4. Click the **Retrieve** subtab.

   The page lists all the retrieved tablespaces.
5. Select and release all the tablespaces.

6.3.3 Verify That the SYS User Is Unlocked and the Password Is Not Expired

If the `sys` password has expired or the `sys` user is locked, you'll receive an error when you run the pre-upgrade RPM during the process of updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

To prevent this issue, update the `sys` user on the primary and standby systems.

1. Perform the following steps on both the primary and standby systems:
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   b. As the `root` user, run the following command:

      ```
      systemctl stop monitor
      ```
   c. Check for any `observerctl` processes running and stop them.

      ```
      ps -elf | grep observerctl
      kill -9 <PID of observerctl>
      ```
   d. Check for any `dgmgrl` processes running and stop them.

      ```
      ps -elf | grep dgmgrl
      kill -9 <PID of dgmgrl>
      ```
2. Update the primary system.
   a. Log in to the primary Audit Vault Server through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

b. Switch to the `oracle` user.

```
su - oracle
```

c. Start SQL*Plus by entering the following command:

```
sqlplus / as sysdba
```

d. Enter the following command:

```
select avsys.secutil.gen_rand_pwd(30) as pwd from dual
```

> **Note:**
>
> Use this password in all steps that require a password on both primary and standby systems.

e. Enter the following commands:

```
alter user sys identified by <password_from_step_1d_above> account
unlock;


ALTER SYSTEM SWITCH LOGFILE;
```

f. Exit back to the `oracle` user.

g. As the `oracle` user, enter the following commands:

```
 mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2_DGMGRL SYS <password_from_step_1d>


mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1_DGMGRL SYS <password_from_step_1d>


mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1 SYS <password_from_step_1d>


mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2 SYS <password_from_step_1d>
```

h. Securely copy the file to the standby system by entering the following command:

```
scp /var/lib/oracle/dbfw/dbs/orapwdbfwdb support@<standby IP>:~/
```

3. Update the standby system.

a. Log in to the standby Audit Vault Server through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

b. Ensure that the new file permissions are the same as the original file.

c. Switch to the `oracle` user.

```
su - oracle
```

d. Enter the following commands:

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2_DGMGRL SYS <password_from_step_1d>
```

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1_DGMGRL SYS <password_from_step_1d>
```

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1 SYS <password_from_step_1d>
```

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2 SYS <password_from_step_1d>
```

4. Enter the following commands as the `root` user on both primary and standby systems:

```
systemctl stop monitor
```

```
systemctl stop dbfwlistener
```

```
systemctl stop dbfwdb
```

```
systemctl start dbfwdb
```

```
systemctl start dbfwlistener
```

```
systemctl start monitor
```

5. Enter the following command as the `oracle` user on both primary and standby systems:

```
/usr/local/dbfw/bin/observerctl --start
```

Related Topics

- Pre-upgrade RPM Fails with "Unable to Stop Observer"
  Learn how to resolve the "unable to stop observer" warning in the pre-upgrade RPM.

6.3.4 Disable FIPS Mode Before Patching to AVDF 20.10

When patching from Oracle AVDF 20.x to 20.10 you first need to disable FIPS mode if it is currently enabled. Once the patch is applied successfully, enable FIPS mode again if required.

To patch AVDF to version 20.10 you must disable the FIPS mode before the patch. The FIPS mode can be enabled once the patch is completed. If the patch is attempted in FIPS mode then the operation will fail with the following message:

```
Precondition: 'fips-mode-check.rb' Result: 'The installed system cannot be
upgraded when the FIPS mode is enabled. Please disable the FIPS mode.'
```

Disable FIPS Mode on the Audit Vault Server

1. Log in to Audit Vault Server console as a `super administrator`.
2. Click the **Settings** tab.
   The **Security** tab in the left navigation menu is selected by default.
3. Click the **FIPS** subtab on the main page.
4. Click the toggle switch to disable FIPS 140-2.
5. Click **Save**.
   A message says that the Audit Vault Server will reboot and prompts you to continue or cancel.
6. Click **OK** to disable FIPS 140-2 for Audit Vault Server. Otherwise, click **Cancel**.

It can take several minutes for the console to become available after disabling FIPS mode.

In a high availability configuration, enabling FIPS 140-2 mode for the primary Audit Vault Server also enables FIPS 140-2 mode for the standby Audit Vault Server. Similarly, disabling FIPS mode for the primary Audit Vault Server also disables it for the standby Audit Vault Server.

Disable FIPS Mode in Database Firewall

- Standalone Database Firewall
- Database Firewall in High Availabilty

Standalone Database Firewall

1. Log in to Audit Vault Server console as `super administrator`.
2. Click **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click the name of the specific Database Firewall instance for which you want to enable FIPS 140-2.
4. Click **FIPS** under the **Configuration** section. A dialog is displayed.
5. In the dialog, turn off the toggle switch to disable FIPS 140-2.
6. Click **Save**. A message pops that Database Firewall will reboot and prompts you to continue or cancel.
7. Click **OK** to continue to disable FIPS 140-2 for the Database Firewall instance. Else, click **Cancel**.
   The Database Firewall instance is restarted and is unavailable for some time.
8. Wait for a while, and navigate back to the **Database Firewalls** tab in the left navigation menu.

9. Check the status of FIPS 140-2 mode under the column **FIPS Mode** against the specific Database Firewall instance.

Database Firewall in High Availabilty

1. Log in to Audit Vault Server console as `super administrator`.
2. Click **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click **High Availability** tab in the left navigation menu. All the Database Firewall instances that are configured in high availability are listed in the main page.
4. The names of paired Database Firewall instances are listed under the **Primary** and **Secondary** columns on the main page. Select the specific pair of Database Firewall instances for which you want to disable FIPS.
5. Click **FIPS** in the top right corner of the page. A dialog is displayed.
6. In the dialog, turn off the toggle switch to disable FIPS 140-2.
7. Click **Save**. A message pops that Database Firewall will reboot and prompts you to continue or cancel.
8. Click **OK** to continue to disable FIPS 140-2 for the Database Firewall instance. Else, click **Cancel**.
   The Database Firewall instance is restarted and is unavailable for some time.
9. Wait for a while, and navigate back to the **Database Firewalls** tab in the left navigation menu.
10. Check the status of FIPS 140-2 mode under the column **FIPS Mode** against the specific Database Firewall instance.

Related Topics

- Enable FIPS Mode If It Was Disabled Before Patching to AVDF 20.10
- Enabling FIPS 140-2 in Oracle AVDF

6.4 Update the Audit Vault Server

Update the Audit Vault Server before you update the Audit Vault Agents and Database Firewalls.

> **Note:**
>
> In this section, the word *appliance* refers to the Audit Vault Server.

6.4.1 Update a Standalone Audit Vault Server

Follow this process to update a standalone Audit Vault Server that is not paired in a high availability environment.

1. Stop all audit trails.

2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers. Don't restart the system while this is in progress.

Update Notes

- If you have existing targets for which you ran Oracle Audit Vault and Database Firewall (Oracle AVDF) setup scripts to set user privileges (for example, for stored procedure auditing), no further action is required to update those privileges after you update Audit Vault Servers.

  Check the Oracle AVDF release notes to find out if you need to rerun the setup scripts because they've changed.
- When updating from Oracle AVDF 12.2 to release 20.1-20.8, password hashing has been upgraded to a more secure standard. This change affects the operating system passwords (support and root). Change your passwords after you update Audit Vault Servers to take advantage of the more secure hash.

6.4.1.1 Stop All Audit Trails

Stop all audit trails before updating the Audit Vault Server.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab.
3. Click **Audit Trails** in the left navigation menu.
4. Select all audit trails.
5. Click **Stop**.

6.4.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.
- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

6.4.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

6.4.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.
3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```
4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

   ```
   Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
   upgrade-20.x.0.0.0.iso
   Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
   Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   ```

```
mount: /dev/loop0 is write-protected, mounting read-only
Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

The following messages have important information about the upgrade process.

Power loss during upgrade may cause data loss. Do not power off during upgrade.
Please review Note ID 2235931.1 for a current list of known issues.

The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
[y/N]?
```

5. Enter `y` to proceed.

   You should see output like the following:

```
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
Verifying upgrade preconditions
1/11: Mounting filesystems (1)
2/11: Cleaning yum configuration
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

6.4.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

```
reboot
```

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.
   c. Select the Database Firewall instance that indicates a certificate error after the update.
   d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

6.4.2 Update a Pair of Audit Vault Servers That Are Configured for High Availability

Follow this process to update a pair of Audit Vault Servers in a high availability environment.

> **Note:**
>
> Don't change the primary and standby roles before completing the update on both Audit Vault Servers.

Follow this process:

1. Update the standby Audit Vault Server.
2. After you reboot the standby Audit Vault Server, ensure that it is up and running before updating the primary Audit Vault Server.
3. Stop the audit trails on the primary Audit Vault Server.
4. Update the primary Audit Vault Server.

   After you reboot the primary Audit Vault Server and confirm that it's running, no additional reboot is needed. It's fully functional at this point.

6.4.2.1 Update the Standby Audit Vault Server

Use this procedure to update the standby Audit Vault Server in a high availability environment. Update the standby Audit Vault server first, then update the primary Audit Vault Server.

Follow this process:

1. Check the failover status on the primary Audit Vault Server.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers. Don't restart the system while this is in progress.

6.4.2.1.1 Check the Failover Status on the Primary Audit Vault Server

Before running the pre-upgrade RPM in a high availability environment, check the failover status on the primary Audit Vault Server. If the failover status is `STALLED`, then wait for a while and check the status again. If the status doesn't change, then contact Oracle Support.

Follow these steps on the primary Audit Vault Server:

1. Log in to the primary Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Run the following command:

   ```
   /usr/local/dbfw/bin/setup_ha.rb --status
   ```
4. Check the failover status in the output.

6.4.2.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the

Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.

- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

6.4.2.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

6.4.2.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```

4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

   ```
   Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
   upgrade-20.x.0.0.0.iso
   Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
   Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   mount: /dev/loop0 is write-protected, mounting read-only
   Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

   The following messages have important information about the upgrade process.

   Power loss during upgrade may cause data loss. Do not power off during upgrade.
   Please review Note ID 2235931.1 for a current list of known issues.

   The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
   [y/N]?
   ```

5. Enter `y` to proceed.

   You should see output like the following:

```
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
Verifying upgrade preconditions
1/11: Mounting filesystems (1)
2/11: Cleaning yum configuration
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

6.4.2.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

```
reboot
```

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:

a. Log in to the Audit Vault Server console as an *administrator*.

b. Click the **Database Firewalls** tab.

   In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.

c. Select the Database Firewall instance that indicates a certificate error after the update.

d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

6.4.2.2 Stop All Audit Trails

Stop all audit trails before updating the Audit Vault Server.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab.
3. Click **Audit Trails** in the left navigation menu.
4. Select all audit trails.
5. Click **Stop**.

6.4.2.3 Update the Primary Audit Vault Server

To update the primary Audit Vault Server in a high availability environment, follow the same process that you used to update the standby Audit Vault Server.

6.5 Verify That Audit Vault Agents and Host Monitor Agents Were Automatically Updated

The Audit Vault Agents and Host Monitor Agents are automatically updated when you update the Audit Vault Server. However, some situations require manual updates.

> **Note:**
>
> During the Audit Vault Agent automatic update process, its status is `UNREACHABLE`. It may take as long as 45 minutes to return to the `RUNNING` state.

In the following situations you may need to update the Audit Vault Agents manually:

- On Windows hosts, the Audit Vault Agent is updated automatically only if you've registered it as a Windows service and you've set this service to use the credentials of the OS user that originally installed the agent. See Additional Requirements for Starting Audit Vault Agent as a Service on Windows for more information.

When you start the agent from the command line, the Audit Vault Agent does not automatically update. In this case, update the agent manually. For example:

```
<agent_home>\bin\agentctl.bat stop
```

Download the new `agent.jar` from the Audit Vault Server console and extract it using `java -jar agent.jar` from the `agent_home` of the existing agent. Then run the following command:

```
<agent_home>\bin\agentctl.bat start
```

Don't delete the existing `agent_home` directory.

- When configuring the Audit vault Server for high availability, if the designated standby Audit Vault Server's agents were deployed before pairing, then manually download and deploy the agents again after pairing.

6.6 Update the Database Firewalls

After you update all Audit Vault Servers, update the Database Firewalls.

When you update Database Firewalls that are configured for high availability (a resilient pair), update both primary and standby Database Firewalls. Update the standby Database Firewall instance first. Restart the standby instance after the update. Swap the roles of the primary and standby Database Firewall instances in the high availability environment so that the existing standby instance becomes the primary instance. Update the standby (previous primary) Database Firewall instance.

For standalone Database Firewall instances, update all of them independently.

Note:

- After updating to Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.3 or later, the status of some of the Database Firewall monitoring points may be `Down`.

  The Database Firewall policies that were created before the update are being migrated to the new format. This may take a few minutes. Navigate to the **Jobs** dialog box in the Audit Vault Server console and check the status of the `Firewall post-upgrade actions` job. If the background job fails, then deploy the Database Firewall policy by using the Audit Vault Server console only. Verify that the status of the Database Firewall monitoring points has changed to `Up`. Otherwise, start the monitoring point.
- You can't perform the following operations until the Database Firewalls are updated:
  - Database Firewall policy deployment
  - New configurations or configuration changes
- In this section, the word *appliance* refers to the Database Firewall.

6.6.1 Update a Standalone Database Firewall

Use this procedure to update a standalone Database Firewall that is not paired in a high availability environment.

Follow this process:

1. Stop all Database Firewall monitoring points.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

6.6.1.1 Stop All Database Firewall Monitoring Points

Stop all monitoring points before updating the Database Firewall.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Click **Database Firewall Monitoring** in the left navigation menu.
4. Select all monitoring points.
5. Click **Stop**.

6.6.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the

Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.

- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

6.6.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

6.6.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```

4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

   ```
   Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
   upgrade-20.x.0.0.0.iso
   Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
   Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   mount: /dev/loop0 is write-protected, mounting read-only
   Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

   The following messages have important information about the upgrade process.

   Power loss during upgrade may cause data loss. Do not power off during upgrade.
   Please review Note ID 2235931.1 for a current list of known issues.
   ```

```
The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
[y/N]?
```

5. Enter `y` to proceed.

   You should see output like the following:

```
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
Verifying upgrade preconditions
1/11: Mounting filesystems (1)
2/11: Cleaning yum configuration
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

6.6.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

```
reboot
```

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.
   c. Select the Database Firewall instance that indicates a certificate error after the update.
   d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

6.6.2 Update a Pair of Database Firewalls That Are Configured for High Availability

Use this procedure to update a pair of Database Firewalls in a high availability environment.

Follow this process:

1. Update the standby Database Firewall.
2. After the standby Database Firewall has fully restarted, swap the standby Database Firewall so that it becomes the primary Database Firewall.
3. Update the original primary (now standby) Database Firewall.
4. (Optional) After the original primary Database Firewall has fully restarted, swap the Database Firewalls so they return to their original primary and standby roles.

6.6.2.1 Update the Standby Database Firewall

Use this procedure to update the standby Database Firewall in a high availability environment. Update the standby Database Firewall first, then swap this Database Firewall so that it becomes the primary Database Firewall. Then update the original primary (now standby) Database Firewall.

Follow this process:

1. Stop all Database Firewall monitoring points.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

6.6.2.1.1 Stop All Database Firewall Monitoring Points

Stop all monitoring points before updating the Database Firewall.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Click **Database Firewall Monitoring** in the left navigation menu.
4. Select all monitoring points.
5. Click **Stop**.

6.6.2.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.
- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

6.6.2.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

6.6.2.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```

4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

   ```
   Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
   upgrade-20.x.0.0.0.iso
   Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
   Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   mount: /dev/loop0 is write-protected, mounting read-only
   Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

   The following messages have important information about the upgrade process.

   Power loss during upgrade may cause data loss. Do not power off during upgrade.
   Please review Note ID 2235931.1 for a current list of known issues.

   The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
   [y/N]?
   ```

5. Enter `y` to proceed.

   You should see output like the following:

   ```
   The Oracle base has been set to /var/lib/oracle
   Error: ORA-01034: ORACLE not available
   ORA-27101: shared memory realm does not exist
   Linux-x86_64 Error: 2: No such file or directory
   Additional information: 4475
   Additional information: 1990413931
   The Oracle base has been set to /var/lib/oracle
   Error: ORA-01034: ORACLE not available
   ORA-27101: shared memory realm does not exist
   Linux-x86_64 Error: 2: No such file or directory
   Additional information: 4475
   Additional information: 1990413931
   Verifying upgrade preconditions
   1/11: Mounting filesystems (1)
   2/11: Cleaning yum configuration
   ```

```
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

6.6.2.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

   ```
   reboot
   ```

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.
   c. Select the Database Firewall instance that indicates a certificate error after the update.
   d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

6.6.2.2 Swap the Standby and Primary Database Firewalls

After updating the standby Database Firewall, swap the standby Database Firewall so that it becomes the primary Database Firewall. You can also swap the Database Firewalls back to their original roles after updating them both.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Click **High Availability** in the left navigation menu.
4. Select this resilient pair of Database Firewall instances.
5. Click **Swap**.

6.6.2.3 Update the Original Primary (Now Standby) Database Firewall

To update the original primary (now standby) Database Firewall in a high availability environment, follow the same process that you used to update the original standby Database Firewall.

6.7 Post-update Tasks

After updating Oracle Audit Vault and Database Firewall (Oracle AVDF), complete these tasks to confirm the update process, enable required functionality, and resolve any remaining issues.

> **Note:**
>
> - If you're updating Audit Vault Server to releases 20.1 through 20.3, then apply the `Deprecated-Cipher-Removal.zip` patch after updating.
> - If you're updating Audit Vault Server to release 20.4 and later, then apply the `Deprecated-Cipher-Removal.zip` patch only if you reduce the TLS level during the update.

> **See Also:**
>
> Unable to Log in to the Oracle AVDF Appliance through SSH

6.7.1 Confirm the Update Process

Use these steps to verify that the update process was successful.

Successful Updates of Audit Vault Servers

1. Verify that you can open the Audit Vault Server console without any issues.
2. Verify that you can log in to the Audit Vault Server console as an *administrator* and an *auditor* without any issues.
3. Verify that you can connect to the Audit Vault Server through SSH without any issues.

4. Log in to the Audit Vault Server console as an *administrator* and check the following items:
   a. Click **Settings** tab, and then click **System** in the left navigation menu.
   b. Verify that the **Audit Vault Server Version** field displays the correct version of Audit Vault Server.
   c. Check the **Uptime** value.
   d. Ensure that **Database Firewall log collection** displays a green arrow pointing up.
   e. Ensure that **Background Job** displays a green arrow pointing up.
   f. Check the **High Availability Status** value.

Successful Updates of Audit Vault Agents

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Agents** tab.
3. Verify that all Audit Vault agents have a status of `RUNNING`.
4. Verify that the **Agent Details** column displays the correct version for each Audit Vault Agent.

Successful Updates of Database Firewalls

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Verify that all Database Firewalls have a status of `Up`.
4. Verify that the **Version** column displays the correct version for each Database Firewall.
5. Click the link for a specific Database Firewall in the **Name** column.
6. Verify that the **Firewall Version** field also displays the correct version.
7. Click the **Health Indicators** link in the **Diagnostics** section and verify that all the health indicators must have a green mark.
8. Close the dialog box.
9. Click **Database Firewall Monitoring** in the left navigation menu.
10. Verify that tall the monitoring points have a status of `Up`.

Unsuccessful Updates

The following symptoms indicate that an update has failed:

- You're unable to open the Audit Vault Server console.
- An SSH connection to the Audit Vault Server (or the terminal) displays an error that the update has failed.

> **Note:**
>
> Also review the system diagnostics for the current status and system log for any errors.

6.7.2 Post Upgrade Agent User Security Hardening

When updating to Oracle Audit Vault and Database Firewall (Oracle AVDF) 20.9 or later, tighten the agent user privileges after all the agents have been updated.

1. Confirm that all the agents have been updated.

   See Confirm the Update Process.

2. Download the `revoke_privileges.sql` script (patch number 35303191) from My Oracle Support.
3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

5. Transfer the downloaded `revoke_privileges.sql` script to the Audit Vault Server (for example, to `/tmp`).
6. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

7. Enter the password at the prompt.
8. Run the `revoke_privileges.sql` script.

   ```
   @<path to revoke_privileges.sql>
   ```

   For example, if you copied the file to `/tmp`, then enter `@/tmp/revoke_privileges.sql`.

9. Exit back to `root`.

   ```
   exit
   ```

10. Lock the `avsys` user.

    See Locking the AVSYS User.

6.7.3 Enable Administrator Access to Existing Archive Locations

After updating Oracle Audit Vault and Database Firewall, the following new behavior applies to archive locations:

- New archive locations are owned by the user with an *administrator* role who created them.
- Users with the *super administrator* role can view all archive locations.
- Only users with the *super administrator* role can access existing archive locations.

To give regular users with the *administrator* role access to existing archive locations, perform the following steps for each archive location:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

3. Exit back to `root`.
4. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

5. Enter the password at the prompt.
6. Run the following commands:

   ```
   update avsys.archive_host set created_by=<adminuser> where name=<archive
   location name>;
   commit;
   exit;
   ```

7. Exit back to `root`.

   ```
   exit
   ```

8. Lock the `avsys` user.

   See Locking the AVSYS User.

6.7.4 Enable Archiving Functionality for High Availability

If the Audit Vault Server is deployed in a high availability environment, you might need to enable archiving after the update.

If you have Network File System (NFS) locations and archived data files, ensure that all the data files are available in the respective NFS locations. After completing the upgrade process, archiving is disabled, so you need to enable it.

- Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.1 and later support archive and retrieve functionality with NFS server versions v3 and v4.
- Only NFS v3 is not supported for releases 20.3 and earlier. It is supported starting Oracle AVDF release 20.4.
- If your NFS server supports and permits both v3 and v4 for archive or retrieve, then no action is required.
- If you have NFS v4 only in your environment for archive or retrieve, then set the `_SHOWMOUNT_DISABLED` parameter to `TRUE` using the following steps:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Start SQL*Plus without the user name or password.

   ```
   sqlplus /nolog
   ```
4. In SQL*Plus, run the following command:

   ```
   connect <super administrator>
   ```
5. Enter the password when prompted.
6. Run the following command:

   ```
   exec avsys.adm.add_config_param('_SHOWMOUNT_DISABLED','TRUE');
   ```

1. Log in to the primary Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Create new NFS locations by using the Audit Vault Server console.

   These new locations consider the newly mounted NFS points for both the primary and secondary Audit Vault Servers. Ensure that there is sufficient space in the newly created NFS locations to store all the necessary data files to be archived.
4. Start SQL*Plus without the user name or password.

   ```
   sqlplus /nolog
   ```
5. In SQL*Plus run the following command:

   ```
   connect super administrator
   ```
6. Enter the password when prompted.
7. Enable the archiving functionality by running the following command:

   ```
   exec management.ar.run_hailm_job('<NFS location name defined>');
   ```

   This command initiates a background job. You can view the status on the Jobs page. The name of the job is `HAILM POST UPGRADE JOB`.

   After you enable this functionality , all the archived data files are moved to the new NFS location and archiving is enabled after the job completes successfully.

6.7.5 Clear Unused Kernels from Oracle Audit Vault and Database Firewall

See My Oracle Support Doc ID 2458154.1 for instructions to clear unused kernels from Oracle Audit Vault and Database Firewall (Oracle AVDF).

6.7.6 Check the Observer Status After Updating to Oracle AVDF 20.7 or Later for High Availability

After upgrading from Oracle AVDF release 20.5 or 20.6 to release 20.7 or later in a high availability environment, you might encounter an issue with the Oracle Data Guard observer. The Audit Vault Server uses Oracle Data Guard to manage high availability.

To check the status of the Oracle Data Guard observer:

1. Log in to the standby Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Run the following commands:

   ```
   dgmgrl /
   ```

   ```
   show observer
   ```

   The output displays the status and the last ping interval of the observers running on both primary and standby Audit Vault Servers. The last ping interval of both observers must have a specific duration in seconds.

4. If the output from the previous step doesn't display a specific duration for both observers, as shown in the following example, then complete the remaining steps to resolve the issue.

   ```
   Host Name:                    <host name>
   Last Ping to Primary:         (unknown)
   Last Ping to Target:          (unknown)
   ```

   a. Log in to the standby Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

   b. Switch to the `oracle` user.

      ```
      su - oracle
      ```

   c. Run the following command:

      ```
      /usr/local/dbfw/bin/observerctl --stop
      ```

   d. Wait for one minute.

e. Run the following commands:

```
dgmgrl /


show observer
```

f. Verify that the last ping interval of both observers has a specific duration in seconds.

6.7.7 Configure Audit Vault Server Backups

The Audit Vault Server backup configuration file is release-specific and works on the same release for which it was created. Oracle recommends that you run the `avbackup config` command to create a new configuration file before performing the backup operation after updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

6.7.8 Schedule Maintenance Jobs

Oracle Audit Vault and Database Firewall (Oracle AVDF) runs some jobs on the Audit Vault Server for proper and effective functioning of the system.

Oracle recommends that you run these jobs during a period when the Audit Vault Server usage is low, such as at night. You can schedule these jobs based on your time zone.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. In the **Configuration** section, click one of the following links, depending on your release:

Oracle AVDF Release	Link
20.1 and 20.2	**Manage**
20.3 and later	**Maintenance**

5. To schedule a new maintenance job, enter the start time in hours and minutes.

   The time that you specify here is the time on the browser.

6. In the **Time Out (In hours)** field, enter the duration of the maintenance job in hours.

   If the job doesn't complete in the specified duration, it times out.

> **Note:**
>
> The job runs at the specified start time daily. You can't change the repeat frequency.

7. Click **Save**.

6.7.9 Enable FIPS Mode If It Was Disabled Before Patching to AVDF 20.10

After successfully patching to Oracle AVDF 20.10, you need to re-enable FIPS mode if it was disabled prior to patching.

Enable FIPS Mode on the Audit Vault Server

1. Log in to Audit Vault Server console as a `super administrator`.
2. Click the **Settings** tab.
   The **Security** tab in the left navigation menu is selected by default.
3. Click the **FIPS** subtab on the main page.
4. Click the toggle switch to enable FIPS 140-2. The toggle switch is green when it's on.
5. Click **Save**.
   A message says that the Audit Vault Server will reboot and prompts you to continue or cancel.
6. Click **OK** to continue to enable FIPS 140-2 for Audit Vault Server. Otherwise, click **Cancel**.

For Oracle AVDF on OCI, if SSH access becomes disabled after enabling FIPS mode, log into the Audit Vault Server console and disable FIPS mode. Then log back into the appliance through SSH and update the user keys for `opc` in `/home/opc/.ssh/authorized_keys` to be compliant with FIPS. It can take several minutes for the console to become available after enabling or disabling FIPS mode.

In a high availability configuration, enabling FIPS 140-2 mode for the primary Audit Vault Server also enables FIPS 140-2 mode for the standby Audit Vault Server. Similarly, disabling FIPS mode for the primary Audit Vault Server also disables it for the standby Audit Vault Server.

Enable FIPS Mode in Database Firewall

- Standalone Database Firewall
- Database Firewall in High Availability

Standalone Database Firewall

1. Log in to Audit Vault Server console as `super administrator`.
2. Click **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click the name of the specific Database Firewall instance for which you want to enable FIPS 140-2.
4. Click **FIPS** under the **Configuration** section. A dialog is displayed.
5. In the dialog, turn on the toggle switch to enable FIPS 140-2. The toggle switch turns green when it is turned on.
6. Click **Save**. A message pops that Database Firewall will reboot and prompts you to continue or cancel.
7. Click **OK** to continue to enable FIPS 140-2 for the Database Firewall instance. Else, click **Cancel**.
   The Database Firewall instance is restarted and is unavailable for some time.

8. Wait for a while, and navigate back to the **Database Firewalls** tab in the left navigation menu.
9. Check the status of FIPS 140-2 mode under the column **FIPS Mode** against the specific Database Firewall instance.

Database Firewall in High Availability

1. Log in to Audit Vault Server console as `super administrator`.
2. Click **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click **High Availability** tab in the left navigation menu. All the Database Firewall instances that are configured in high availability are listed in the main page.
4. The names of paired Database Firewall instances are listed under the **Primary** and **Secondary** columns on the main page. Select the specific pair of Database Firewall instances for which you want to enable FIPS.
5. Click **FIPS** in the top right corner of the page. A dialog is displayed.
6. Turn on the toggle switch to enable FIPS 140-2. The toggle switch turns green when it is turned on.
7. Click **Save** button. A message pops that the Database Firewall instances will reboot and prompts you to continue or cancel.
8. Click **OK** to continue to enable FIPS 140-2 for the Database Firewall instances. Else, click **Cancel**.
   The Database Firewall instances are restarted and are unavailable for some time.
9. Wait for a while and check the status of FIPS 140-2 mode under the column **FIPS Mode** against the paired Database Firewall instances.

Related Topics

- Disable FIPS Mode Before Patching to AVDF 20.10
- Enabling FIPS 140-2 in Oracle AVDF

6.7.10 Update Alert Notification Template for Alert Policies After Patching to AVDF 20.11

After successfully patching to Oracle AVDF 20.11, you need to update the alert notification template for your alert policies.

After patching to Oracle AVDF 20.11, the alert notification template for existing alert policies will be set to the default alert template. Auditors may need to update the alert notification template for their alert policies.

For more information on modifying email templates, see Creating or Modifying an Email Template in Oracle's Audit Vault and Database Firewall Auditor's Guide.

6.7.11 Retrieve Audit Policies After Patching to 20.12

After successfully patching to Oracle AVDF 20.12, you need to retrieve audit policies on your Oracle databases.

After patching to Oracle AVDF 20.12, an auditor will need to retrieve audit policies again on any Oracle databases.

For more information on retrieving audit policies, see Retrieving and Modifying Audit Policies from an Oracle Database in the *Oracle Audit Vault and Database Firewall Auditor's Guide*.

6.8 Recover the Database If an Update Fails

If you backed up Oracle Audit Vault and Database Firewall (Oracle AVDF) before updating, and if there is enough space in the Audit Vault Server's flash recovery area, you may be able to recover the database after a failed update under the guidance of Oracle Support.

To make recovery of the database possible, you should have the following amount of free space in the flash recovery area:

20 GB or 150% of the amount of data that is stored in the Audit Vault Server database, whichever is larger

For information on monitoring the flash recovery area, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

6.9 Updating Oracle AVDF with Minimal Downtime by Using Backup and Restore

You can use the backup and restore functionality to update Oracle Audit Vault and Database Firewall (Oracle AVDF) to a new release with minimal downtime for monitoring and collecting data.

You can use this process to update from Oracle AVDF 20.3 and later to release 20.9 and later.

6.9.1 About the Update Process

When you update the Audit Vault Server to the latest Oracle AVDF release, you normally stop monitoring and collecting audit data at the beginning of the update process, which causes downtime until you complete the full update process.

To minimize this downtime, you can continue monitoring and collecting with your current (**source**) Audit Vault Server while performing the update on a new (**destination**) Audit Vault Server that's a backup-restored system. The source Audit Vault Server continues to monitor and collect audit data during the update. When the destination Audit Vault Server is completely updated, you migrate the delta data and then switch monitoring from the source Audit Vault Server to the new destination.

To update Oracle AVDF with the backup and restore functionality, use the following high-level process:

1. Configure the source and destination Audit Vault Servers.
2. Create a hot backup of the source Audit Vault Server.
3. Restore the hot backup to the destination Audit Vault Server.
4. Update the destination Audit Vault Server to the latest release.
5. For a high availability environment, pair the primary and standby Audit Vault Servers.
6. Replicate the collected audit data from the source Audit Vault Server to the destination.
7. Update and migrate all monitoring and collection to the destination Audit Vault Server.

8. Start all audit trails on the destination Audit Vault Server.

To perform the update process, complete all the tasks under this section.

6.9.2 Prerequisites

Complete the following tasks before beginning the update process.

1. For the destination Audit Vault Server, complete a fresh installation of Oracle AVDF with the same hardware configuration as the current (source) Audit Vault Server.

   Install the same Oracle AVDF release that's running on the source Audit Vault Server. You'll update to the new Oracle AVDF release after you back up and restore to the destination Audit Vault Server.

   See Downloading and Installing Oracle Audit Vault and Database Firewall for instructions.
2. Ensure that the new destination Audit Vault Server can access and connect to the source Audit Vault Server.

6.9.3 Configure the Source and Destination Audit Vault Servers

Before beginning the backup and restore process, you need to configure the source and destination Audit Vault Servers to be able to replicate the collected audit data later in the update process.

This configuration creates and starts the Oracle GoldenGate processes that will perform the data replication. You perform the actual replication later, after you update the destination Audit Vault Server to the latest release.

To configure the source and destination Audit Vault Servers, complete all the tasks under this section.

> **Note:**
>
> If, at any point during the update process, you need to change the destination Audit Vault Server or uninstall or reinstall the patch from the destination Audit Vault Server, uninstall the patch from the source Audit Vault Server and restart the update process from the beginning. For the patch bug numbers for your release, see Patch Bug Numbers for the Source and Destination Audit Vault Servers.

6.9.3.1 Patch Bug Numbers for the Source and Destination Audit Vault Servers

As part of the configuration, you install patches on the source and destination Audit Vault Servers.

Download both source and destination Audit Vault Server patches for your Oracle AVDF release.

Table 6-1 Patch Bug Numbers for the Source Audit Vault Server

Target Oracle AVDF Release	Patch Bug Number
Updating to 20.13	37474251
Updating to 20.12	36782027

Table 6-1 (Cont.) Patch Bug Numbers for the Source Audit Vault Server

Target Oracle AVDF Release	Patch Bug Number
Updating to 20.11	36290747
Updating to 20.10	35703285
Updating to 20.9	34625846

Table 6-2 Patch Bug Numbers for the Destination Audit Vault Server

Target Oracle AVDF Release	Patch Bug Number
Updating to 20.13	37474256
Updating to 20.12	36782032
Updating to 20.11	36290752
Updating to 20.10	35703288
Updating to 20.9	34625855

6.9.3.2 Create an NFS Location as an Archive Log Destination for the Source Audit Vault Server

Create a Network File System (NFS) location to use as the archive log destination for the Source Audit Vault Server.

1. Log in to the source Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Monitor the space used for the archive logs.

   a. Switch to the `oracle` user.

   ```
   su - oracle
   ```

   b. Start SQL*Plus as `sysdba`.

   ```
   sqlplus / as sysdba
   ```

   c. Run the following query:

   ```
   select  sum( blocks*block_size)/1024/1024 "Size (MB)" from
   v$archived_log where DELETED = 'NO';
   ```

   This query shows the space usage for the archive logs.

> **Note:**
>
> Use this query to monitor the size of archive log on source Audit Vault Server throughout the next steps. If the query output exceeds the size of the NFS location that you mount on the source Audit Vault Server in the following steps, add more space to the NFS location.

d. Exit SQL*Plus.

```
exit
```

3. Mount an NFS location that has at least 500 GB free space on the source Audit Vault Server.
   a. Create a directory to use as a mount point (for example, `/archive_log`).
   b. Run the following command (using `/archive_log` as an example):

```
mount -t nfs <NFS_IP>:<export_path> /archive_log
```

      The exact `mount` command may vary.

      Make sure that the `oracle` user has `read`, `write`, and `execute` permissions for the directory that you created as the mount point.

      If you updated `/etc/fstab` to add the mount point, it reverts to the original state when the system is restarted.

4. Set `log_archive_dest_1` to the mounted NFS location.
   a. Switch to the `oracle` user.

```
su - oracle
```

   b. Start SQL*Plus as `sysdba`.

```
sqlplus / as sysdba
```

   c. Run the following command (using `/archive_log` as an example):

```
alter system set log_archive_dest_1='LOCATION=/archive_log' scope=both;
```

   d. Exit SQL*Plus.

```
exit
```

6.9.3.3 Configure the Source Audit Vault Server for Replication

Before you back up the source Audit Vault Server, you need to configure it for replication.

This is required to replicate the data that was collected during the update process from the source Audit Vault Server to the destination Audit Vault Server.

> **Note:**
>
> For a high availability configuration, apply this patch only on the primary Audit Vault Server.

1. From My Oracle Support, download the source Audit Vault Server patch for your release. See Patch Bug Numbers for the Source and Destination Audit Vault Servers.

2. Securely copy `avs-source-20.x-replication.rpm` to `/home/support/` on the source Audit Vault Server.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, copy the file to `/home/opc/`.

3. Log in to the source Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. As the `root` user, install the RPM.

```
mv /home/support/avs-source-20.x-replication.rpm /


rpm -i /avs-source-20.x-replication.rpm
```

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, enter the following commands:
>
> ```
> mv /home/opc/avs-source-20.x-replication.rpm /
>
>
> rpm -i /avs-source-20.x-replication.rpm
> ```

5. Switch to the `oracle` user.

```
su - oracle
```

6. Run `AVS_source_data_replication.py`.

   a. Enter the following command:

```
/usr/bin/python /var/lib/oracle/avs_source/
AVS_source_data_replication.py --configure
```

      This command creates a new replication user, `GGADMINSRC`.

   b. When prompted, enter a new password for the `GGADMINSRC` user.

      The password should have at least one uppercase letter, one letter, one number, and one special character. It should be between 8 and 30 characters.

      You'll also need this password when you configure the destination Audit Vault Server for replication later in this process.

   c. When prompted, enter the super administrator user name and password.

   If the installation is successful, you should see the following message:

```
AVS configured as source for replication successfully.
```

If you don't see this message, contact Oracle Support.

7. If you receive a warning message that archive log mode is not enabled, enable archive log mode before the next step.

   To enable archive log mode, follow these steps:

   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

   b. Run the following command to stop the monitor process:

      ```
      systemctl stop monitor
      ```

   c. Run the following command to shut down the Audit Vault Server repository (Oracle Database):

      ```
      systemctl stop dbfwdb
      ```

   d. Run the following command to ensure that the Audit Vault Server repository is shut down:

      ```
      /usr/local/dbfw/bin/dbfwdb status
      ```

      The output is `ORACLE instance shut down.`

   e. Switch to the `oracle` user.

      ```
      su - oracle
      ```

   f. Start SQL*Plus as `sysdba`.

      ```
      sqlplus / as sysdba
      ```

   g. Run the following commands at the SQL*Plus prompt to enable archive log mode:

      ```
      startup mount

      alter database archivelog;

      alter database open;

      shutdown immediate;
      ```

   h. Exit SQL*Plus.

      ```
      exit
      ```

8. Run the following command to start the Audit Vault Server repository (Oracle Database):

   ```
   systemctl start dbfwdb
   ```

9. Run the following command to start the monitor process:

```
systemctl start monitor
```

10. As the `root` user, switch to the `dvowner` user and grant the replication privilege to the new replication user, `GGADMINSRC`.

```
su dvowner


sqlplus /


grant DV_GOLDENGATE_ADMIN, DV_GOLDENGATE_REDO_ACCESS to GGADMINSRC;
```

6.9.3.4 Configure the Destination Audit Vault Server for Replication

Before you back up the source Audit Vault Server and restore it to the destination Audit Vault Server, you need to configure it for replication.

This is required to replicate the data that was collected during the update process from the source Audit Vault Server to the destination Audit Vault Server.

1. From My Oracle Support, download the destination Audit Vault Server patch for your release. See Patch Bug Numbers for the Source and Destination Audit Vault Servers.
2. Securely copy `avs-destination-20.x-replication.rpm` to `/home/support/` on the destination Audit Vault Server.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, copy the file to `/home/opc/`.

3. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
4. As the `root` user, install the RPM.

```
mv /home/support/avs-destination-20.x-replication.rpm /


rpm -i avs-destination-20.x-replication.rpm
```

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, enter the following commands:
>
> ```
> mv /home/opc/avs-destination-20.x-replication.rpm /
>
> rpm -i avs-destination-20.x-replication.rpm
> ```

5. Switch to the `oracle` user.

   ```
   su - oracle
   ```

6. Verify that archive log mode is disabled.

   a. Start SQL*Plus as `sysdba`.

      ```
      sqlplus / as sysdba
      ```

   b. Enter the following command to verify the archive log mode:

      ```
      select log_mode from v$database;
      ```

      If the output is `NOARCHIVELOG`, then archive log mode is disabled.

      If the output is `ARCHIVELOG`, then archive log mode is enabled and you need to disable it.

   c. To disable archive log mode, enter the following commands in sequence as the `oracle` user:

      ```
      shutdown immediate;

      startup mount;

      alter database noarchivelog;

      alter database open;
      ```

   d. Verify that the changes were made.

      ```
      select name,log_mode from v$database;
      ```

      The output should be `NOARCHIVELOG`.

7. Run the following command:

```
/usr/bin/python /var/lib/oracle/avs_goldengate/
AVS_target_data_replication.py --install_and_configure
```

   This command installs the Oracle GoldenGate Microservices Architecture.

8. When prompted, enter a password for the new GoldenGate user, `AVS_GG_ADMIN`, that's created.

   The password should have at least one uppercase letter, one letter, one number, and one special character. It should be between 8 and 30 characters.

   You'll also need this password later in the replication process.

9. When prompted, enter the IP address and the password for the `GGADMINSRC` user.

   You created this password when you configured the source Audit Vault Server for replication in the following step: Configure the Source Audit Vault Server for Replication.

   If the installation is successful, you should see the following message:

   ```
   AVS configured as destination for replication successfully.
   ```

   If you don't see this message, contact Oracle Support.

   > **Note:**
   >
   > To see all available commands, run the following command:
   >
   > ```
   > /usr/bin/python /var/lib/oracle/avs_goldengate/AVS_tar
   > get_data_replication.py --help
   > ```

10. Mount the `/var/lib/oracle/avs_goldengate/avs_goldengate_dep/var/lib/data` directory to an NFS location with at least 500 GB of available free space.

    This is different from the NFS location that's mounted on the source Audit Vault Server.

    Run the following command:

    ```
    mount -t nfs <NFS_IP>:<export_path> /var/lib/oracle/avs_goldengate/
    avs_goldengate_dep/var/lib/data
    ```

    The exact `mount` command may vary.

    Make sure that the `oracle` user has `read`, `write`, and `execute` permissions for the directory that you created as the mount point.

    If you updated `/etc/fstab` to add the mount point, it reverts to the original state when the system is restarted.

11. Mount the same NFS location that you mounted and used for archive logs on the source Audit Vault Server, with the exact same mount point path.

    This is the same NFS location that you set up in the following step: Create an NFS Location as an Archive Log Destination for the Source Audit Vault Server.

12. As the `oracle` user, enter the following commands:

```
rman target /


CONFIGURE ARCHIVELOG DELETION POLICY TO BACKED UP 5 TIMES to disk;
```

6.9.4 Create a Hot Backup of the Source Audit Vault Server

Perform a hot (or hot incremental) backup of the source Audit Vault Server to the Network File System (NFS) location that you configured earlier in this process.

Use the NFS location that you configured in the following step: Create an NFS Location as an Archive Log Destination for the Source Audit Vault Server.

The destination Audit Vault Server must be able to access this NFS backup location.

When performing the backup, set the `REDUNDANCY` to `2`.

See Backup and Restore of Audit Vault Server for the full instructions.

> **Note:**
>
> For a high availability configuration, back up the primary Audit Vault Server and restore it to a standalone system.

6.9.5 Restore the Hot Backup to the Destination Audit Vault Server

Restore from the hot backup of the source Audit Vault Server to the destination Audit Vault Server.

Restore from the NFS location that you backed up to in the following step: Create a Hot Backup of the Source Audit Vault Server.

Set the `USE_NEW_IP` option to yes (`USE_NEW_IP: Y`).

See Restoring from Audit Vault Server Backup for instructions.

> **Note:**
>
> Don't perform the post-restore tasks after you complete the restore process.

6.9.6 Set the Archive Log Destination on the Destination Audit Vault Server

Before proceeding with the update to Oracle AVDF 20.9, set `log_archive_dest_1` on the destination Audit Vault Server.

1. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

```
su - oracle
```

3. Start SQL*Plus as `sysdba`.

```
sqlplus / as sysdba
```

4. Enter the following command:

```
alter system set log_archive_dest_1='LOCATION=+RECOVERY' scope=both;
```

5. Exit SQL*Plus.

```
exit
```

6.9.7 Update the Destination Audit Vault Server to the Latest Release

After you back up the source Audit Vault Server and restore it to the destination Audit Vault Server, you update the destination Audit Vault Server to the latest release (Oracle AVDF 20.9 or later).

See Patching Oracle Audit Vault and Database Firewall Release 20 for instructions.

6.9.8 (High Availability Only) Pair the Primary and Standby Audit Vault Servers

After the update is complete, pair the Audit Vault Servers for high availability.

Use the destination Audit Vault Server as the primary server and perform a fresh install of the latest version of Oracle AVDF on the standby Audit Vault Server.

For instructions, see Configuring High Availability for Audit Vault Servers.

Related Topics

- Downloading and Installing Oracle Audit Vault and Database Firewall
  Learn how to download and install Oracle Audit Vault and Database Firewall (Oracle AVDF).

6.9.9 Replicate the Data That Was Collected During the Update Process

After you've updated the destination Audit Vault Server to the latest release, you need to replicate the data that was collected on the source Audit Vault Server during the update process to the destination Audit Vault Server.

To replicate the data that was collected during the updated process, complete all the tasks under this section.

6.9.9.1 Start the Replication on the Destination Audit Vault Server

To start the replication script on the destination Audit Vault Server, provide the complete path to the backup directory on the destination Audit Vault Server. This is the same path that you specified when you restored the hot backup to the destination Audit Vault Server.

> **Note:**
>
> In a high availability environment, complete these steps on the primary Audit Vault Server.

Prerequisite

Ensure that the backup directory and the `/var/lib/oracle/avs_goldengate/avs_goldengate_dep/var/lib/data` directory are mounted on the destination Audit Vault Server. For details, see Configure the Source and Destination Audit Vault Servers.

Procedure

1. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Enter the following command:

   ```
   /usr/bin/python2 /var/lib/oracle/avs_goldengate/
   AVS_target_data_replication.py --start <backup_directory>
   ```

   Provide the complete path to the backup directory on the destination Audit Vault Server. This is the same path that you specified when backing up and restoring to the destination Audit Vault Server in the following steps: Create a Hot Backup of the Source Audit Vault Server and Restore the Hot Backup to the Destination Audit Vault Server.

4. When prompted, enter the password for the `AVS_GG_ADMIN` user.

   This is the password that you created when you installed the patch in the destination Audit Vault Server in the following step: Configure the Destination Audit Vault Server for Replication.

6.9.9.2 Check the Replication Status on the Destination Audit Vault Server

To ensure that the replication is running, check the replication status on the destination Audit Vault Server.

> **Note:**
>
> In a high availability environment, complete these steps on the primary Audit Vault Server.

1. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Enter the following command:

```
/usr/bin/python2 /var/lib/oracle/avs_goldengate/
AVS_target_data_replication.py --check_replication_status
```

The status should be `Running` for both `extract` and `replicat`. If it's not `Running` for both, contact Oracle Support.

6.9.9.3 Set Up the Purge Task on the Destination Audit Vault Server

While the replication is running, set up the purge task on the destination Audit Vault Server to automatically purge Oracle GoldenGate trail files that were created during replication.

> **Note:**
>
> In a high availability environment, complete these steps on the primary Audit Vault Server.

1. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

```
su - oracle
```

3. Enter the following command:

```
/usr/bin/python2 /var/lib/oracle/avs_goldengate/
AVS_target_data_replication.py --setup_purge_task
```

4. When prompted, enter the password for the `AVS_GG_ADMIN` user.

   You created this password when you configured the destination Audit Vault Server for replication in the following step: Configure the Destination Audit Vault Server for Replication.

6.9.9.4 Check the Replication Lag Time on the Destination Audit Vault Server

Before you stop monitoring points and audit trails on the source Audit Vault Server, ensure that the replication lag time on the destination server is less than 60 seconds.

> **Note:**
>
> In a high availability environment, complete these steps on the primary Audit Vault Server.

1. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

```
su - oracle
```

3. Enter the following command:

```
/usr/bin/python2 /var/lib/oracle/avs_goldengate/
AVS_target_data_replication.py --check_replication_lag
```

You should see output in the following format:

```
Processing Lag: <time> seconds
Extract lag: <time> seconds
Replicat lag: <time> seconds
```

6.9.9.5 Stop All Monitoring Points and Audit Trails on the Source Audit Vault Server

When all replication lag times are less than 60 seconds, stop all monitoring points and audit trails on the source Audit Vault Server.

To check the lag time, see Check the Replication Lag Time on the Destination Audit Vault Server.

To stop monitoring points, see Starting, Stopping, or Deleting Database Firewall Monitoring Points.

To stop audit trails, see Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server.

6.9.9.6 Stop the Replication on the Destination Audit Vault Server

When the replication lag is 0 seconds, stop the data replication on the the destination Audit Vault Server.

> **Note:**
>
> In a high availability environment, complete these steps on the primary Audit Vault Server.

To check the lag time, see Check the Replication Lag Time on the Destination Audit Vault Server. You should see the following results before proceeding:

```
Processing Lag: 0 seconds
Extract records processed. No lag.
Replicat records processed. No lag.
```

To stop the replication:

1. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

```
su - oracle
```

3. Enter the following command:

```
/usr/bin/python2 /var/lib/oracle/avs_goldengate/
AVS_target_data_replication.py --stop
```

4. After stopping, enter the following command and ensure that the replication status is `Stopped`.

```
/usr/bin/python2 /var/lib/oracle/avs_goldengate/
AVS_target_data_replication.py --check_replication_status
```

6.9.10 Update and Migrate All Monitoring and Collection to the Destination Audit Vault Server

After the data replication is complete, update and migrate all Database Firewalls and Audit Vault Agents to the destination Audit Vault Server.

Prerequisites

If the source Audit Vault Server release was 20.3, 20.4, 20.5, or 20.6, ensure that the patch for bug 34676006 has been applied on the source Audit Vault Server.

If the source Audit Vault Server release was 20.1 - 20.9 ensure that the patch for bug 35997720 has been applied on the destination Audit Vault Server.

Procedure

1. Update and migrate Database Firewalls by completing the following steps for each firewall:
   a. Update the Database Firewall to the latest release.

      See Patching Oracle Audit Vault and Database Firewall Release 20.
   b. Reassociate the Database Firewall with the destination Audit Vault Server's IP address.

      See Specifying the Audit Vault Server Certificate and IP Address.
   c. Reset the Database Firewall from the destination Audit Vault Server.

      See Resetting Database Firewall.
   d. In the destination Audit Vault Server console, ensure that the version of the Database Firewall shows the updated release (20.9 or later).
2. Update and migrate Audit Vault Agents and Host Monitor Agents by running the agent update script on the source Audit Vault Server.
   a. Log in to the source Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   b. Switch to the `oracle` user.

      ```
      su - oracle
      ```

   c. Enter the following command:

      ```
      sh /var/lib/oracle/avs_source/send_agent_migration_signal.sh  -
      primary_avs <ip_of_destination_primary_or_standalone_AVS>  [-
      ```

```
standby_avs <ip_of_destination_standby_AVS>] [-tcpport <tcp  port def
1521>] [-tcpsport <tcps port def 2484>]
```

d. Verify that the agents are successfully updated.

   In the destination Audit Vault Server console, the agents should be in the `RUNNING` state. If they're not, contact Oracle Support.

Postrequisite

If the source Audit Vault Server release was 20.1 - 20.9 and patch 35997720 was applied, then remove the patch from the destination Audit Vault Server.

6.9.11 Start All Audit Trails on the Destination Audit Vault Server

After the Database Firewalls and Audit Vault Agents are updated and migrated to the destination Audit Vault Server, start all audit trails on the destination Audit Vault Server.

For instructions, see Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server.

It may take up to 20 minutes for the audit trails to start running.

At this point, all monitoring and connections should be from the destination Audit Vault Server. The source Audit Vault Server has old data and can be decommissioned.

6.9.12 Uninstall the Replication Patches from the Source and Destination Audit Vault Servers

When the update is complete and data has been replicated to the destination Audit Vault Server, you can uninstall the replication patches from the source and destination Audit Vault Servers.

1. Uninstall the patch from the source Audit Vault Server.

   For the patch bug numbers for your release, see Patch Bug Numbers for the Source and Destination Audit Vault Servers.

   a. Log in to the source Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

   b. Switch to the `oracle` user.

      ```
      su - oracle
      ```

   c. Run the following command:

      ```
      /usr/bin/python /var/lib/oracle/avs_source/
      AVS_source_data_replication.py --unconfigure
      ```

2. When prompted, enter the super administrator user name and password.
3. As the `root` user, uninstall the RPM.

   ```
   rpm -e $(rpm -qa | grep avs-source)
   ```

4. Uninstall the patch from the destination Audit Vault Server.

For the patch bug numbers for your release, see Patch Bug Numbers for the Source and Destination Audit Vault Servers.

> **Note:**
>
> In a high availability environment, complete these steps on the primary Audit Vault Server.

> **Note:**
>
> Before uninstalling the patch, ensure that the following command was run:
>
> ```
> /usr/bin/python2 /var/lib/oracle/avs_goldengate/
> AVS_target_data_replication.py --stop
> ```
>
> For details, see the following step: Stop the Replication on the Destination Audit Vault Server.

a. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

b. Unmount the file system.

   ```
   /bin/umount /var/lib/oracle/avs_goldengate/avs_goldengate_dep/var/lib/
   data
   ```

c. Switch to the `oracle` user.

   ```
   su - oracle
   ```

d. Run the following command:

   ```
   /usr/bin/python2 /var/lib/oracle/avs_goldengate/
   AVS_target_data_replication.py --remove_users_and_uninstall
   ```

e. When prompted, enter the super administrator user name and password.

f. As the `root` user, uninstall the RPM.

   ```
   rpm -e $(rpm -qa | grep avs-destination)
   ```

7

Upgrading Oracle Audit Vault and Database Firewall from Release 12.2 to Release 20

If you're on Oracle Audit Vault and Database Firewall (Oracle AVDF) release 12.2, you can upgrade to release 20 to maintain support and access the latest features and bug fixes.

If you're already on Oracle AVDF release 20, see Patching Oracle Audit Vault and Database Firewall Release 20 to apply the latest release updates.

> **Note:**
>
> This chapter uses the terms *update* and *upgrade* interchangeable.

7.1 About Upgrading Oracle Audit Vault and Database Firewall

Follow these guidelines for upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF) release 12.2 to release 20.

Use the following high-level process to upgrade Oracle AVDF:

1. Download the files from My Oracle Support.
2. Complete the pre-update tasks, such as creating a backup.
3. Update the Audit Vault Servers.
4. Verify that Audit Vault Agents and Host Monitor Agents were updated automatically.
5. Update the Database Firewalls.
6. Complete the post-update tasks, such as confirming that the update was successful.

> **Note:**
>
> - To upgrade Oracle AVDF from release 12.2 to release 20.9 or later, first upgrade to release 20.8 and then apply the latest release update (RU) patch.
> - If you're on Oracle AVDF 12.2.0.0.0 to 12.2.0.8.0, upgrade to release 12.2.0.9.0 before upgrading to release 20.
>
>   You can perform a single backup operation before performing the first upgrade.
> - If you've deployed Database Firewall In-line Bridge mode in release 12.2, follow the instructions in Change the Database Firewall In-line Bridge to an Equivalent Proxy Configuration.
> - If you have a large amount of event data, maintain sufficient disk space of about 5% of the total event log data size.
>
>   If you have both HDD and SAN storage, then maintain the necessary disk space on either HDD or SAN. Each disk group (EVENTDATA, SYSTEMDATA, and RECOVERY) should have at least 20% available space.

7.2 Upgrading from Oracle AVDF 12.2 to Release 20.8

Follow this process to upgrade Oracle Audit Vault and Database Firewall (Oracle AVDF) from release 12.2 to release 20.8.

7.2.1 Download the Files

To patch or upgrade Oracle Audit Vault and Database firewall (Oracle AVDF), you need to download files from My Oracle Support.

1. Go to My Oracle Support and sign in.
2. Click the **Patches & Updates** tab.
3. Use the **Patch Search** box to search for the patch.
   a. Click the **Product or Family (Advanced)** link on the left.
   b. In the **Product** field, enter *Audit Vault and Database Firewall*.
   c. In the **Release** field, select the latest Oracle AVDF release from the drop-down list.
   d. Click **Search**.
4. In the **Patch Name** column of the search results, click the link for the latest bundle patch.

7.2.2 Pre-update Tasks

Before updating Oracle Audit Vault and Database Firewall (Oracle AVDF) to the latest release, complete the prerequisite tasks, such as performing a backup.

> **Note:**
>
> If Audit Vault Agent is running on a Windows machine, close all the agent-related directories and open files before updating Oracle AVDF.

7.2.2.1 Migrate Host Monitor Agent on Windows

If you're on Oracle Audit Vault and Database Firewall (Oracle AVDF) release 12.2 and you use Host Monitoring on Windows, then update the Npcap and OpenSSL libraries on Windows before upgrading to Oracle AVDF release 20.

Complete the following tasks:

- After installing Npcap and OpenSSL, ensure that the `network_device_name_for_hostmonitor` collection attribute is set.

  See Create a Network Audit Trail for instructions.
- Deploying the Host Monitor Agent on a Windows Host Machine

7.2.2.2 Back Up the Current Oracle Audit Vault and Database Firewall Installation

Before updating Oracle Audit Vault and Database Firewall (Oracle AVDF) to the latest release, back up the Audit Vault Server.

See Backing Up and Restoring the Audit Vault Server for complete information.

If your current Audit Vault Server is installed on a virtual machine (VM), such as Oracle VM or VMWare, Oracle recommends that you take a VM snapshot before starting the update process.

7.2.2.3 Set the Host Monitor Agent and Audit Vault Agent TLS Version

If your current Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 deployment has Host Monitor Agents or Audit Vault Agents on AIX and you're upgrading to Oracle AVDF 20.4 or later, set the TLS version to TLS 1.1 before upgrading.

If you're upgrading from Oracle AVDF 12.2.0.11.0 and earlier and you've deployed Host Monitor Agents (or Audit Vault Agents on AIX) with the default version of TLS 1.2, the Host Monitor Agents (or Audit Vault Agents on AIX) do not upgrade automatically.

For Oracle AVDF 12.2.0.12.0 and later, this issue only affects Audit Vault Agents on AIX.

To prevent this issue, run the following command before upgrading:

```
ruby /usr/local/dbfw/bin/upgrade/configure_tls_settings.rb 2
```

> **Note:**
>
> After upgrading, set the TLS level to *Level-4*. See Post Upgrade TLS Security Hardening for more information.

Related Topics

- Pre-upgrade RPM Check: Legacy Crypto Warning
  If your current Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 deployment has Host Monitor Agents or Audit Vault Agents on AIX and you're upgrading to Oracle AVDF 20.4 or later, then the pre-upgrade RPM displays a warning about TLS and encryption.

7.2.2.4 Ensure That the System Has Sufficient Space to Purge the Alert Queue

If the system doesn't have sufficient space to purge the alert queue, you'll receive an error when you run the pre-upgrade RPM during the process of updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

Follow these steps to prevent this issue:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

3. Exit back to `root`.
4. Switch to the `oracle` user.

   ```
   su - oracle
   ```

5. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

6. Enter the password at the prompt.
7. Run the following SQL query:

   ```
   declare object_exist exception; pragma exception_init(object_exist,
   -24002); po dbms_aqadm.aq$_purge_options_t;
   begin po.block := FALSE; dbms_aqadm.purge_queue_table('AVSYS.AV_ALERT_QT',
   NULL, po);
   exception when object_exist then null; end;/
   ```

8. Exit back to `root`.

   ```
   exit
   ```

9. Lock the `avsys` user.

   See Locking the AVSYS User.

Related Topics

- Pre-upgrade RPM Check: Alert Queue Space Warning
  The pre-upgrade RPM displays a warning if the system doesn't have sufficient space to purge the alert queue during the upgrade.

7.2.2.5 Release Existing Tablespaces That Are Retrieved Manually

If you're updating to Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.1 through 20.3, release all the existing tablespaces that were retrieved manually. This procedure is performed automatically if you're updating to Oracle AVDF release 20.4 or later.

The following steps are only applicable for AVDF 20.1 - 20.3.

If you don't release the existing tablespaces, the following situations could occur:

- The update might fail, resulting in an error.
- New indexes might not be created after the update because space can't be allocated.

To manually release the tablespaces, follow these steps:

1. Log in to the Audit Vault Server console as a *super administrator*.
2. Click the **Settings** tab.
3. Click **Archiving** in the left navigation menu.
4. Click the **Retrieve** subtab.

   The page lists all the retrieved tablespaces.
5. Select and release all the tablespaces.

7.2.2.6 Preserve File Customizations

Preserve customizations that have been applied to configuration files before upgrading to Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.

The upgrade erases all custom changes that have been made to system configuration files. Oracle recommends that you back up any required changes that you need to transfer to the upgraded system.

To preserve file customizations:

- Create your own custom configuration file. See the *Oracle Linux* documentation for details.
- Move any rules to a custom configuration file before performing the upgrade process.
- Synchronize the time between the Database Firewalls and Audit Vault Servers.

  If the system clocks for the Database Firewalls and Audit Vault Servers are not synchronized, then you may see a certificate error after the upgrade. After the upgrade, check the appliance diagnostics output to ensure that everything is marked `OK` in green. The diagnostic failures are marked `FAILED` in red.

  – To configure the time for Audit Vault Servers, see Specifying the Server Date, Time, and Keyboard Settings.
- To configure the time for Database Firewalls, see Setting the Date and Time in Oracle Database Firewall.

7.2.2.7 Ensure That the Boot Device Is Less Than 2 TB

If the boot device is greater than 2 TB, you'll receive an error when you run the pre-upgrade RPM during the process of upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF).

Boot Device Is Greater Than 2 TB When Upgrading the Audit Vault Server

Follow these steps if the boot device is greater than 2 TB when upgrading the Audit Vault Server:

1. Stop all trails and monitoring points.
2. Stop all Audit Vault Agents and shut down all Database Firewall servers.
3. Back up the system.
4. Choose a server that has at least one hard disk that is less than 2 TB.
5. Install the same bundle patch version of Audit Vault Server on release 12.2.
6. Configure the system to boot in BIOS mode.
7. Restore from the backup. Use the same IP address and ensure that the system is up.
8. Upgrade the Audit Vault Server to release 20 using the documented upgrade process.

Boot Device Is Greater Than 2 TB When Upgrading a Database Firewall That Was Added to the Audit Vault Server Before Release 12.2.0.1.0

1. Reset the Database Firewall.
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click **Reset Firewall** to update all the settings on the Audit Vault Server.
2. Choose a server that has at least one hard disk that is less than 2 TB.
3. Install the same bundle patch version of Database Firewall on release 12.2.
4. Configure the system to boot in BIOS mode.
5. Log in to the Audit Vault Server console as an *administrator*.
6. Configure the Database Firewall instance.
7. Specify the Audit Vault Server certificate and IP address on the new Database Firewall instance.
8. Click the **Database Firewalls** tab.

   The status of the newly installed Database Firewall instance is `Down` (red).
9. Click the name of the specific Database Firewall instance.
10. Click **Update Certificate**, and wait for the page to load.

    The status of the Database Firewall instance is `Up` (green).
11. Click **Reset Firewall**.
12. Click **OK**.
13. Check the status of this operation in the **Jobs** dialog box.
    a. Click the **Settings** tab.
    b. Click **System** in the left navigation menu.

c. Click the **Jobs** link in the **Monitoring** section.

   The job type is `Reset Firewall`.

14. Click the **Job Details** page icon on the left.

    If the job has failed, a message appears in the **Job Status Details** dialog box. If the job is successful, then it displays the completion time.

Boot Device Is Greater Than 2 TB When Upgrading a Database Firewall on Oracle AVDF 12.2.0.2.0 or Later

1. Choose a server that has at least one hard disk that is less than 2 TB.
2. Install the same bundle patch version of Database Firewall on release 12.2.
3. Configure the system to boot in BIOS mode.
4. Log in to the Audit Vault Server console as an *administrator*.
5. Configure the Database Firewall instance.
6. Specify the Audit Vault Server certificate and IP address on the new Database Firewall instance.
7. Click the **Database Firewalls** tab.

   The status of the newly installed Database Firewall instance is `Down` (red).
8. Click the name of the specific Database Firewall instance.
9. Click **Update Certificate**, and wait for the page to load.

   The status of the Database Firewall instance is `Up` (green).
10. Click **Reset Firewall**.
11. Click **OK**.
12. Check the status of this operation in the **Jobs** dialog box.
    a. Click the **Settings** tab.
    b. Click **System** in the left navigation menu.
    c. Click the **Jobs** link in the **Monitoring** section.

       The job type is `Reset Firewall`.
13. Click the **Job Details** page icon on the left.

    If the job has failed, a message appears in the **Job Status Details** dialog box. If the job is successful, then it displays the completion time.

Related Topics

- Pre-upgrade RPM Check: Boot Device Is Greater Than 2 TB
  The pre-upgrade RPM warns you if the boot device greater than 2 TB, in which case the upgrade process may fail. Ensure that the boot device is less than 2 TB before upgrading.

7.2.2.8 Ensure That the Boot Partition Has at Least 500 MB

If the boot partition has less than 500 MB, you'll receive an error when you run the pre-upgrade RPM during the process of updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

Insufficient Space in the Boot Partition When Upgrading the Audit Vault Server

Follow these steps if there is insufficient space in the boot partition when upgrading the Audit Vault Server:

1. Stop all trails and monitoring points.
2. Stop all Audit Vault Agents and shut down all Database Firewall servers.
3. Back up of the system.
4. Install the same bundle patch version of Audit Vault Server on release 12.2.

   This creates the `/boot` partition with 500 MB.
5. Restore from the backup. Use the same IP address and ensure that the system is up.
6. Upgrade Audit Vault Server to release 20 using the documented upgrade process.

Insufficient Space in the Boot Partition When Upgrading a Database Firewall

Follow these steps if there is insufficient space in the boot partition when upgrading a Database Firewall:

1. If the Database Firewall was added to the Audit Vault Server before release 12.2.0.1.0, reset the Database Firewall.
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click **Reset Firewall** to update all the settings on the Audit Vault Server.
2. Install the same bundle patch version of Database Firewall on release 12.2. This creates the `/boot` partition with 500 MB.
3. Log in to the Audit Vault Server console as an *administrator*.
4. Configure the Database Firewall instance.
5. Specify the Audit Vault Server certificate and IP address on the new Database Firewall instance.
6. Click the **Database Firewalls**tab.

   The status of the newly installed Database Firewall instance is `Down` (red).
7. Click the name of the specific Database Firewall instance.
8. Click **Update Certificate**, and wait for the page to load.

   The status of the Database Firewall instance is `Up` (green).
9. Click **Reset Firewall**.
10. Click **OK**.
11. Check the status of this operation in the **Jobs** dialog box.
    a. Click the **Settings** tab.
    b. Click **System** in the left navigation menu.
    c. Click the **Jobs** link in the **Monitoring** section.

The job type is `Reset Firewall`.

12. Click the **Job Details** page icon on the left.

    If the job has failed, a message appears in the **Job Status Details** dialog box. If the job is successful, then it displays the completion time.

13. Check the overall health status of the Database Firewall instance.
    a. Click the **Database Firewalls** tab.
    b. Click the name of the specific instance.
    c. Click the **Health Indicators** link in the **Diagnostics** section.

14. Expand the **Certificates** section.

    Check the message about certificate validation failure, and take appropriate action.

15. Expand the **Database Firewall Monitoring** section and ensure that all statuses are green.

16. Click **Close**.

Related Topics

- Pre-upgrade RPM Check: Boot Partition Space Warning
  The pre-upgrade RPM warns you if there is not enough space in the boot partition, in which case the upgrade process may fail. Ensure that the boot partition has at least 500 MB before upgrading.

7.2.2.9 Verify That the SYS User Is Unlocked and the Password Is Not Expired

If the `sys` password has expired or the `sys` user is locked, you'll receive an error when you run the pre-upgrade RPM during the process of updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

To prevent this issue, update the `sys` user on the primary and standby systems.

1. Perform the following steps on both the primary and standby systems:
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

   b. As the `root` user, run the following command:

      ```
      systemctl stop monitor
      ```

   c. Check for any `observerctl` processes running and stop them.

      ```
      ps -elf | grep observerctl
      kill -9 <PID of observerctl>
      ```

   d. Check for any `dgmgrl` processes running and stop them.

      ```
      ps -elf | grep dgmgrl
      kill -9 <PID of dgmgrl>
      ```

2. Update the primary system.
   a. Log in to the primary Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

b. Switch to the `oracle` user.

```
su - oracle
```

c. Start SQL*Plus by entering the following command:

```
sqlplus / as sysdba
```

d. Enter the following command:

```
select avsys.secutil.gen_rand_pwd(30) as pwd from dual
```

> **Note:**
>
> Use this password in all steps that require a password on both primary and standby systems.

e. Enter the following commands:

```
alter user sys identified by <password_from_step_1d_above> account
unlock;


ALTER SYSTEM SWITCH LOGFILE;
```

f. Exit back to the `oracle` user.

g. As the `oracle` user, enter the following commands:

```
 mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2_DGMGRL SYS <password_from_step_1d>


mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1_DGMGRL SYS <password_from_step_1d>


mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1 SYS <password_from_step_1d>


mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2 SYS <password_from_step_1d>
```

h. Securely copy the file to the standby system by entering the following command:

```
scp /var/lib/oracle/dbfw/dbs/orapwdbfwdb support@<standby IP>:~/
```

3. Update the standby system.

a. Log in to the standby Audit Vault Server through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

b. Ensure that the new file permissions are the same as the original file.

c. Switch to the `oracle` user.

```
su - oracle
```

d. Enter the following commands:

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2_DGMGRL SYS <password_from_step_1d>
```

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1_DGMGRL SYS <password_from_step_1d>
```

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA1 SYS <password_from_step_1d>
```

```
mkstore -wrl /var/lib/oracle/dbfw/network/admin/observer/ -
modifyCredential DBFWDB_HA2 SYS <password_from_step_1d>
```

4. Enter the following commands as the `root` user on both primary and standby systems:

```
systemctl stop monitor
```

```
systemctl stop dbfwlistener
```

```
systemctl stop dbfwdb
```

```
systemctl start dbfwdb
```

```
systemctl start dbfwlistener
```

```
systemctl start monitor
```

5. Enter the following command as the `oracle` user on both primary and standby systems:

```
/usr/local/dbfw/bin/observerctl --start
```

Related Topics

- Pre-upgrade RPM Fails with "Unable to Stop Observer"
  Learn how to resolve the "unable to stop observer" warning in the pre-upgrade RPM.

7.2.3 Update the Audit Vault Server

Update the Audit Vault Server before you update the Audit Vault Agents and Database Firewalls.

> **Note:**
>
> In this section, the word *appliance* refers to the Audit Vault Server.

7.2.3.1 Update a Standalone Audit Vault Server

Follow this process to update a standalone Audit Vault Server that is not paired in a high availability environment.

1. Stop all audit trails.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers. Don't restart the system while this is in progress.

Update Notes

- If you have existing targets for which you ran Oracle Audit Vault and Database Firewall (Oracle AVDF) setup scripts to set user privileges (for example, for stored procedure auditing), no further action is required to update those privileges after you update Audit Vault Servers.

  Check the Oracle AVDF release notes to find out if you need to rerun the setup scripts because they've changed.
- When updating from Oracle AVDF 12.2 to release 20.1-20.8, password hashing has been upgraded to a more secure standard. This change affects the operating system passwords (support and root). Change your passwords after you update Audit Vault Servers to take advantage of the more secure hash.

7.2.3.1.1 Stop All Audit Trails

Stop all audit trails before updating the Audit Vault Server.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab.
3. Click **Audit Trails** in the left navigation menu.
4. Select all audit trails.
5. Click **Stop**.

7.2.3.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.
- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

```
SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
The upgrade can then be started by running: /usr/bin/avdf-upgrade
```

If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

7.2.3.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

7.2.3.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.
3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```
4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

```
Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
upgrade-20.x.0.0.0.iso
Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
mount: /dev/loop0 is write-protected, mounting read-only
Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

The following messages have important information about the upgrade process.

Power loss during upgrade may cause data loss. Do not power off during upgrade.
Please review Note ID 2235931.1 for a current list of known issues.

The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
[y/N]?
```

5. Enter `y` to proceed.

   You should see output like the following:

```
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
Verifying upgrade preconditions
1/11: Mounting filesystems (1)
2/11: Cleaning yum configuration
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

7.2.3.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

```
reboot
```

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.
   c. Select the Database Firewall instance that indicates a certificate error after the update.
   d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

7.2.3.2 Update a Pair of Audit Vault Servers That Are Configured for High Availability

Follow this process to update a pair of Audit Vault Servers in a high availability environment.

> **Note:**
>
> Don't change the primary and standby roles before completing the update on both Audit Vault Servers.

Follow this process:

1. Update the standby Audit Vault Server.
2. After you reboot the standby Audit Vault Server, ensure that it is up and running before updating the primary Audit Vault Server.
3. Stop the audit trails on the primary Audit Vault Server.
4. Update the primary Audit Vault Server.

   After you reboot the primary Audit Vault Server and confirm that it's running, no additional reboot is needed. It's fully functional at this point.

7.2.3.2.1 Update the Standby Audit Vault Server

Use this procedure to update the standby Audit Vault Server in a high availability environment. Update the standby Audit Vault server first, then update the primary Audit Vault Server.

Follow this process:

1. Check the failover status on the primary Audit Vault Server.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers. Don't restart the system while this is in progress.

7.2.3.2.1.1 Check the Failover Status on the Primary Audit Vault Server

Before running the pre-upgrade RPM in a high availability environment, check the failover status on the primary Audit Vault Server. If the failover status is `STALLED`, then wait for a while and check the status again. If the status doesn't change, then contact Oracle Support.

Follow these steps on the primary Audit Vault Server:

1. Log in to the primary Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Run the following command:

   ```
   /usr/local/dbfw/bin/setup_ha.rb --status
   ```

4. Check the failover status in the output.

7.2.3.2.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.
- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

7.2.3.2.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

7.2.3.2.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```

4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

   ```
   Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
   upgrade-20.x.0.0.0.iso
   Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
   Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   mount: /dev/loop0 is write-protected, mounting read-only
   ```

```
Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

The following messages have important information about the upgrade process.

Power loss during upgrade may cause data loss. Do not power off during upgrade.
Please review Note ID 2235931.1 for a current list of known issues.

The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
[y/N]?
```

5. Enter `y` to proceed.

   You should see output like the following:

```
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
Verifying upgrade preconditions
1/11: Mounting filesystems (1)
2/11: Cleaning yum configuration
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

7.2.3.2.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

```
reboot
```

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.
   c. Select the Database Firewall instance that indicates a certificate error after the update.
   d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

7.2.3.2.2 Stop All Audit Trails

Stop all audit trails before updating the Audit Vault Server.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab.
3. Click **Audit Trails** in the left navigation menu.
4. Select all audit trails.
5. Click **Stop**.

7.2.3.2.3 Update the Primary Audit Vault Server

To update the primary Audit Vault Server in a high availability environment, follow the same process that you used to update the standby Audit Vault Server.

7.2.4 Verify That Audit Vault Agents and Host Monitor Agents Were Automatically Updated

The Audit Vault Agents and Host Monitor Agents are automatically updated when you update the Audit Vault Server. However, some situations require manual updates.

> **Note:**
>
> During the Audit Vault Agent automatic update process, its status is `UNREACHABLE`. It may take as long as 45 minutes to return to the `RUNNING` state.

In the following situations you may need to update the Audit Vault Agents manually:

- On Windows hosts, the Audit Vault Agent is updated automatically only if you've registered it as a Windows service and you've set this service to use the credentials of the OS user that originally installed the agent. See Additional Requirements for Starting Audit Vault Agent as a Service on Windows for more information.

  When you start the agent from the command line, the Audit Vault Agent does not automatically update. In this case, update the agent manually. For example:

  ```
  <agent_home>\bin\agentctl.bat stop
  ```

  Download the new `agent.jar` from the Audit Vault Server console and extract it using `java -jar agent.jar` from the `agent_home` of the existing agent. Then run the following command:

  ```
  <agent_home>\bin\agentctl.bat start
  ```

  Don't delete the existing `agent_home` directory.

- When configuring the Audit vault Server for high availability, if the designated standby Audit Vault Server's agents were deployed before pairing, then manually download and deploy the agents again after pairing.

7.2.5 Update the Database Firewalls

After you update all Audit Vault Servers, update the Database Firewalls.

When you update Database Firewalls that are configured for high availability (a resilient pair), update both primary and standby Database Firewalls. Update the standby Database Firewall instance first. Restart the standby instance after the update. Swap the roles of the primary and standby Database Firewall instances in the high availability environment so that the existing standby instance becomes the primary instance. Update the standby (previous primary) Database Firewall instance.

For standalone Database Firewall instances, update all of them independently.

> **Note:**
>
> - After updating to Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.3 or later, the status of some of the Database Firewall monitoring points may be `Down`.
>
> The Database Firewall policies that were created before the update are being migrated to the new format. This may take a few minutes. Navigate to the **Jobs** dialog box in the Audit Vault Server console and check the status of the `Firewall post-upgrade actions` job. If the background job fails, then deploy the Database Firewall policy by using the Audit Vault Server console only. Verify that the status of the Database Firewall monitoring points has changed to `Up`. Otherwise, start the monitoring point.
> - You can't perform the following operations until the Database Firewalls are updated:
> – Database Firewall policy deployment
> – New configurations or configuration changes
> - In this section, the word *appliance* refers to the Database Firewall.

7.2.5.1 Update a Standalone Database Firewall

Use this procedure to update a standalone Database Firewall that is not paired in a high availability environment.

Follow this process:

1. Stop all Database Firewall monitoring points.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

7.2.5.1.1 Stop All Database Firewall Monitoring Points

Stop all monitoring points before updating the Database Firewall.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Click **Database Firewall Monitoring** in the left navigation menu.
4. Select all monitoring points.

5. Click **Stop**.

7.2.5.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.
- Verifies that other prerequisites and platform conditions are met before the update.
- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

7.2.5.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

   ```
   scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
   ```

7.2.5.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Run the following command to perform the appropriate checks before updating:

   ```
   /usr/bin/avdf-upgrade
   ```

4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

   ```
   Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
   upgrade-20.x.0.0.0.iso
   Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
   Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   mount: /dev/loop0 is write-protected, mounting read-only
   Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

   The following messages have important information about the upgrade process.

   Power loss during upgrade may cause data loss. Do not power off during upgrade.
   Please review Note ID 2235931.1 for a current list of known issues.

   The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
   [y/N]?
   ```

5. Enter `y` to proceed.

   You should see output like the following:

   ```
   The Oracle base has been set to /var/lib/oracle
   Error: ORA-01034: ORACLE not available
   ORA-27101: shared memory realm does not exist
   Linux-x86_64 Error: 2: No such file or directory
   Additional information: 4475
   Additional information: 1990413931
   The Oracle base has been set to /var/lib/oracle
   Error: ORA-01034: ORACLE not available
   ORA-27101: shared memory realm does not exist
   Linux-x86_64 Error: 2: No such file or directory
   Additional information: 4475
   Additional information: 1990413931
   Verifying upgrade preconditions
   1/11: Mounting filesystems (1)
   2/11: Cleaning yum configuration
   3/11: Cleaning old packages and files
   4/11: Upgrading kernel
   5/11: Upgrading system
   6/11: Cleaning platform packages repo
   7/11: Adding required platform packages
   8/11: Cleaning AVDF packages repo
   9/11: Installing AVDF packages
   10/11: Setting boot title
   11/11: Setting final system status
   Reboot now to continue the upgrade process.
   Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
   ```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

7.2.5.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

   ```
   reboot
   ```

   > **Note:**
   >
   > When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:
   a. Log in to the Audit Vault Server console as an *administrator*.
   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.
   c. Select the Database Firewall instance that indicates a certificate error after the update.
   d. Click **Reset Firewall**.

   > **See Also:**
   >
   > Registering a Database Firewall in the Audit Vault Server

7.2.5.2 Update a Pair of Database Firewalls That Are Configured for High Availability

Use this procedure to update a pair of Database Firewalls in a high availability environment.

Follow this process:

1. Update the standby Database Firewall.
2. After the standby Database Firewall has fully restarted, swap the standby Database Firewall so that it becomes the primary Database Firewall.
3. Update the original primary (now standby) Database Firewall.
4. (Optional) After the original primary Database Firewall has fully restarted, swap the Database Firewalls so they return to their original primary and standby roles.

7.2.5.2.1 Update the Standby Database Firewall

Use this procedure to update the standby Database Firewall in a high availability environment. Update the standby Database Firewall first, then swap this Database Firewall so that it

becomes the primary Database Firewall. Then update the original primary (now standby) Database Firewall.

Follow this process:

1. Stop all Database Firewall monitoring points.
2. Run the pre-upgrade RPM.
3. Transfer the ISO file to the appliance.
4. Start the update script.
5. Restart the appliance.

> **Note:**
>
> When the appliance restarts, the update process continues. This takes several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

7.2.5.2.1.1 Stop All Database Firewall Monitoring Points

Stop all monitoring points before updating the Database Firewall.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Click **Database Firewall Monitoring** in the left navigation menu.
4. Select all monitoring points.
5. Click **Stop**.

7.2.5.2.1.2 Run the Pre-upgrade RPM

Run the pre-upgrade RPM to check for the required space in the file system and prepare the system for updating.

> **Note:**
>
> The patching process uses the same pre-upgrade RPM as the upgrade process, although patching involves a smaller subset of tasks compared to a full upgrade.

The pre-upgrade RPM performs the following tasks to prepare the system for updating:

- Rearranges free space on the appliance so that there's enough room to copy the patch files to the appliance and start the installation. After the update, the space for the patch files is returned to the file system.
- Starting with updates from Oracle AVDF 20.9 to Oracle AVDF 20.10 and later, verifies that the Audit Vault Agents and Host Monitor Agents are compatible with the new version of the Audit Vault Server. For example, it verifies that agent host machines have compatible operating system and Java versions.
- Verifies that other prerequisites and platform conditions are met before the update.

- Prepares the system for updating by creating the `/var/dbfw/upgrade` directory with enough space to hold the main ISO file for the update.

To run the pre-upgrade RPM, follow these steps:

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Change to the `root` directory.

   ```
   cd /root
   ```

4. Run the following command to copy the pre-upgrade RPM file from the downloaded location to the appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-20.x.0.0.0.zip /root
   ```

5. Verify the download by using a shasum of the `avdf-pre-upgrade-20.x.0.0.0.zip` file.

   ```
   sha256sum /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

6. Unzip the bundle.

   ```
   unzip /root/avdf-pre-upgrade-20.x.0.0.0.zip
   ```

7. Run the following command to run the `avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm` file:

   ```
   rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
   ```

   The following message appears:

   ```
   SUCCESS: The upgrade media can now be copied to '/var/dbfw/upgrade'.
   The upgrade can then be started by running: /usr/bin/avdf-upgrade
   ```

   If you receive any errors instead of a `SUCCESS` message, resolve them before proceeding.

Related Topics

- Pre-upgrade RPM Warnings
  While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.
- Upgrade From AVDF 20.9 On an OCI Audit Vault Server Doesn't Have Enough Free Space

7.2.5.2.1.3 Transfer the ISO File to the Appliance

Transfer the `avdf-upgrade-20.x.0.0.0.iso` file to the appliance that you're updating.

1. Log in to the appliance through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

2. Copy the `avdf-upgrade-20.x.0.0.0.iso` file by using the following command:

```
scp remote_host:/path/to/avdf-upgrade-20.x.0.0.0.iso /var/dbfw/upgrade
```

7.2.5.2.1.4 Start the Update Script

The update script mounts the ISO, changes to the correct working directory, runs the update process, and unmounts the ISO after the upgrade process is complete.

> **Note:**
>
> The system may take some time to complete the commands. Don't interrupt the update or the system may be left in an inconsistent state. For this reason, it is important to use a reliable and uninterruptible shell, such as a direct console login (or ILOM equivalent), or use the `screen` command to prevent network disconnections from interrupting the update.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the `screen` command as the `root` user.

   The `screen` command prevents network disconnections from interrupting the update. If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

3. Run the following command to perform the appropriate checks before updating:

```
/usr/bin/avdf-upgrade
```

4. Follow the system prompt, warning, and instruction to proceed with the update accordingly.

   You should see output like the following:

```
Please wait while validating SHA256 checksum for /var/dbfw/upgrade/avdf-
upgrade-20.x.0.0.0.iso
Checksum validation successful for /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso
Mounting /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
mount: /dev/loop0 is write-protected, mounting read-only
Successfully mounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images

The following messages have important information about the upgrade process.

Power loss during upgrade may cause data loss. Do not power off during upgrade.
Please review Note ID 2235931.1 for a current list of known issues.

The upgrade process is irreversible, please confirm 'y' to continue or 'n' to abort.
[y/N]?
```

5. Enter `y` to proceed.

   You should see output like the following:

```
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
```

```
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
The Oracle base has been set to /var/lib/oracle
Error: ORA-01034: ORACLE not available
ORA-27101: shared memory realm does not exist
Linux-x86_64 Error: 2: No such file or directory
Additional information: 4475
Additional information: 1990413931
Verifying upgrade preconditions
1/11: Mounting filesystems (1)
2/11: Cleaning yum configuration
3/11: Cleaning old packages and files
4/11: Upgrading kernel
5/11: Upgrading system
6/11: Cleaning platform packages repo
7/11: Adding required platform packages
8/11: Cleaning AVDF packages repo
9/11: Installing AVDF packages
10/11: Setting boot title
11/11: Setting final system status
Reboot now to continue the upgrade process.
Unmounted /var/dbfw/upgrade/avdf-upgrade-20.x.0.0.0.iso on /images
```

> **Note:**
>
> The preceding output varies depending on the base installation level, appliance type, and configuration.

7.2.5.2.1.5 Restart the Appliance

After updating, restart the appliance and continue the update process.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Restart the appliance. For example:

   ```
   reboot
   ```

   > **Note:**
   >
   > When the appliance restarts, the update process continues. This takes several hours to complete on Audit Vault Servers and several minutes to complete on Database Firewalls. Don't restart the system while this is in progress.

3. If you've updated a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to reregister the Database Firewall. To check this:

   a. Log in to the Audit Vault Server console as an *administrator*.

   b. Click the **Database Firewalls** tab.

      In the left navigation menu, **Database Firewalls** is selected by default and the page displays a list of configured Database Firewall instances.

c. Select the Database Firewall instance that indicates a certificate error after the update.

d. Click **Reset Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

7.2.5.2.2 Swap the Standby and Primary Database Firewalls

After updating the standby Database Firewall, swap the standby Database Firewall so that it becomes the primary Database Firewall. You can also swap the Database Firewalls back to their original roles after updating them both.

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Click **High Availability** in the left navigation menu.
4. Select this resilient pair of Database Firewall instances.
5. Click **Swap**.

7.2.5.2.3 Update the Original Primary (Now Standby) Database Firewall

To update the original primary (now standby) Database Firewall in a high availability environment, follow the same process that you used to update the original standby Database Firewall.

7.2.6 Post-update Tasks

After updating Oracle Audit Vault and Database Firewall (Oracle AVDF), complete these tasks to confirm the update process, enable required functionality, and resolve any remaining issues.

> **Note:**
>
> - If you're updating Audit Vault Server to releases 20.1 through 20.3, then apply the `Deprecated-Cipher-Removal.zip` patch after updating.
> - If you're updating Audit Vault Server to release 20.4 and later, then apply the `Deprecated-Cipher-Removal.zip` patch only if you reduce the TLS level during the update.

> **See Also:**
>
> Unable to Log in to the Oracle AVDF Appliance through SSH

7.2.6.1 Confirm the Update Process

Use these steps to verify that the update process was successful.

Successful Updates of Audit Vault Servers

1. Verify that you can open the Audit Vault Server console without any issues.
2. Verify that you can log in to the Audit Vault Server console as an *administrator* and an *auditor* without any issues.
3. Verify that you can connect to the Audit Vault Server through SSH without any issues.
4. Log in to the Audit Vault Server console as an *administrator* and check the following items:
   a. Click **Settings** tab, and then click **System** in the left navigation menu.
   b. Verify that the **Audit Vault Server Version** field displays the correct version of Audit Vault Server.
   c. Check the **Uptime** value.
   d. Ensure that **Database Firewall log collection** displays a green arrow pointing up.
   e. Ensure that **Background Job** displays a green arrow pointing up.
   f. Check the **High Availability Status** value.

Successful Updates of Audit Vault Agents

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Agents** tab.
3. Verify that all Audit Vault agents have a status of `RUNNING`.
4. Verify that the **Agent Details** column displays the correct version for each Audit Vault Agent.

Successful Updates of Database Firewalls

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Verify that all Database Firewalls have a status of `Up`.
4. Verify that the **Version** column displays the correct version for each Database Firewall.
5. Click the link for a specific Database Firewall in the **Name** column.
6. Verify that the **Firewall Version** field also displays the correct version.
7. Click the **Health Indicators** link in the **Diagnostics** section and verify that all the health indicators must have a green mark.
8. Close the dialog box.
9. Click **Database Firewall Monitoring** in the left navigation menu.
10. Verify that tall the monitoring points have a status of `Up`.

Unsuccessful Updates

The following symptoms indicate that an update has failed:

- You're unable to open the Audit Vault Server console.

- An SSH connection to the Audit Vault Server (or the terminal) displays an error that the update has failed.

> **Note:**
>
> Also review the system diagnostics for the current status and system log for any errors.

7.2.6.2 Post Upgrade TLS Security Hardening

If your previous Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 deployment had Host Monitor Agents or Audit Vault Agents on AIX and you upgraded to Oracle AVDF 20.4 or later, then you set the TLS version to TLS 1.1 before upgrading. After upgrading, you should reset the TLS level.

If you set the TLS version to TLS 1.1 before upgrading, as discussed in the following topics, then the upgrade process did not automatically set the TLS level to *Level-4*:

- Set the Host Monitor Agent and Audit Vault Agent TLS Version
- Pre-upgrade RPM Check: Legacy Crypto Warning

After the update process is complete (including all agents), Oracle strongly recommends setting the TLS level to *Level-4*. See About Setting Transport Layer Security Levels for instructions.

7.2.6.3 Post Upgrade Agent User Security Hardening

When updating to Oracle Audit Vault and Database Firewall (Oracle AVDF) 20.9 or later, tighten the agent user privileges after all the agents have been updated.

1. Confirm that all the agents have been updated.

   See Confirm the Update Process.

2. Download the `revoke_privileges.sql` script (patch number 35303191) from My Oracle Support.
3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

5. Transfer the downloaded `revoke_privileges.sql` script to the Audit Vault Server (for example, to `/tmp`).
6. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

7. Enter the password at the prompt.
8. Run the `revoke_privileges.sql` script.

   ```
   @<path to revoke_privileges.sql>
   ```

   For example, if you copied the file to `/tmp`, then enter `@/tmp/revoke_privileges.sql`.
9. Exit back to `root`.

   ```
   exit
   ```

10. Lock the `avsys` user.

    See Locking the AVSYS User.

7.2.6.4 Add Preexisting SQL Clusters to New Cluster Sets After Upgrading

After upgrading to Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20, you can't add preexisting SQL clusters from release 12.2 to new cluster sets when creating new Database Firewall policies.

To resolve this issue, run the `populate_cluster_job.sql` script immediately after upgrading to Oracle AVDF release 20. This script resolves the issue in the event log table and you can create cluster sets based on the clusters that were generated before the upgrade to 20.1.

> **Note:**
>
> This issue occurs in Oracle AVDF 20.1 only. It is resolved in later releases.

1. Download the `populate_cluster_job.sql` script from ARU or My Oracle Support.
2. (Optional) Stop the Database Firewall monitoring points and other traffic.

   This is not required, but doing so makes the script run faster.

   See Starting, Stopping, or Deleting Database Firewall Monitoring Points.
3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
4. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

5. Exit back to `root`.
6. Switch to the `oracle` user.

   ```
   su - oracle
   ```

7. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

8. Enter the password at the prompt.
9. Run the following script:

   ```
   @<file path of the populate_cluster_job.sql script>
   ```

   The script runs in the background. The duration of the script is based on the traffic, and sometimes it takes longer.
10. Check the status of the job.
    a. Log in to the Audit Vault Server console as an *administrator*.
    b. Click the **Settings** tab.
    c. Click **System** in the left navigation menu.
    d. Click **Jobs**.

       The status of the job type is *Retrieve_clusters*.
    e. If the script failed, repeat the preceding steps to run the script again.
11. Exit back to `root`.

    ```
    exit
    ```

12. Lock the `avsys` user.

    See Locking the AVSYS User.

7.2.6.5 Change the Database Firewall In-line Bridge to an Equivalent Proxy Configuration

The Database Firewall In-line Bridge deployment mode is desupported in Oracle AVDF release 20. If you have Database Firewall In-line Bridge mode deployed in release 12.2, you need to update your configuration to an equivalent proxy mode. The deprecation notice was issued in release 12.2.

Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20 requires configuration changes to maintain network separation that was originally provided by a traffic source (bridge). The order of the network interface cards (NIC) and the components that are connected can't be determined.

> **Note:**
>
> A single proxy port is required for every target. A single proxy port can't service multiple target databases. Add more traffic proxy ports as required.

Complete this task if you meet the following conditions:

- The current Database Firewall is on Oracle AVDF release 12.2.

- The Database Firewall is currently deployed in monitoring (DAM) or blocking (DPE) mode with one or more traffic sources that are configured as a bridge.
- You want to maintain your existing network segmentation.
- The interfaces are used for monitoring only.
- The default bridge device is created or repurposed to create the monitoring point services.

To update your configuration to an equivalent proxy mode:

1. Complete the upgrade to Oracle AVDF release 20.

   After the upgrade, the NICs have the original bridge configuration.

2. Log in to the Audit Vault Server console to check the current status of the Database Firewall network configuration.

   From the available Database Firewall configuration information, the network connections of the two interfaces that are used by the traffic source are not known.

3. Determine the information of the network segment and the interfaces that plugged in by using a tool like ping.

4. Determine which of the two NICs is the client-side NIC, make a note, and ensure that the device has a valid IP address and is up.

   > **Note:**
   >
   > Be sure to add a valid proxy port for this interface. A default port number is created automatically.

5. Determine which of the two NICs is the database-facing NIC, make a note, and ensure that the device has a valid IP address and is up.

6. After collecting the required data and reviewing the Database Firewall configuration, ping the target addresses from the database-facing device.

7. Enable one NIC at a time and attempt to ping the target addresses from the appliance.

   If you can't find any information on the first interface, then check on the second one. If the target addresses are not available, then try pinging the local gateway. This approach usually directs towards the clients.

   Assuming that no other network changes are made, the network mask remains the same.

   After you enable the NICs and incorporate the changes, the settings in the `NET_SERVICE_MAP` within the `dbfw.conf` file are similar to the following:

   ```
   NET_SERVICE_MAP="{"enp0s9":{"ip4":
   {"address":"192.0.2.21/24","gateway":"","enabled":true}},"enp0s10":{"ip4":
   {"address":"192.0.2.20/24","gateway":"","enabled":true}}}"
   ```

8. Add the routes to the NET_SERVICE_MAP as follows.

   Routes are required so that the proxy can send the traffic between the clients and the database.

   ```
   NET_SERVICE_MAP="{"enp0s9":{"ip4":
   {"address":"192.0.2.21/24","gateway":"","enabled":true},'route':
   {'ip4route':['192.0.2.4/22 192.0.2.21',...]}},...}
   ```

The routing requires a general range for the clients as follows:

```
ip route add 192.0.2.21/24 via 192.0.2.20 dev enp0s10
```

The routing range for the targets is as follows:

```
ip route add 192.0.2.4 via 192.0.2.21 dev enp0s9
```

9. Run the following command to apply all the settings:

```
configure-networking
```

10. Test the client connectivity with the database.

Related Topics

- Configuring Database Firewall as a Traffic Proxy
- Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.1

7.2.6.6 Enable Administrator Access to Existing Archive Locations

After updating Oracle Audit Vault and Database Firewall, the following new behavior applies to archive locations:

- New archive locations are owned by the user with an *administrator* role who created them.
- Users with the *super administrator* role can view all archive locations.
- Only users with the *super administrator* role can access existing archive locations.

To give regular users with the *administrator* role access to existing archive locations, perform the following steps for each archive location:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

> **Note:**
>
> Remember to relock the `avsys` account when you've completed this task.

3. Exit back to `root`.
4. Start SQL*Plus as the `avsys` user.

```
sqlplus avsys
```

5. Enter the password at the prompt.
6. Run the following commands:

```
update avsys.archive_host set created_by=<adminuser> where name=<archive
location name>;
```

```
commit;
exit;
```

7. Exit back to `root`.

   ```
   exit
   ```

8. Lock the `avsys` user.

   See Locking the AVSYS User.

7.2.6.7 Enable Archiving Functionality for High Availability

If the Audit Vault Server is deployed in a high availability environment, you might need to enable archiving after the update.

If you have Network File System (NFS) locations and archived data files, ensure that all the data files are available in the respective NFS locations. After completing the upgrade process, archiving is disabled, so you need to enable it.

- Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.1 and later support archive and retrieve functionality with NFS server versions v3 and v4.
- Only NFS v3 is not supported for releases 20.3 and earlier. It is supported starting Oracle AVDF release 20.4.
- If your NFS server supports and permits both v3 and v4 for archive or retrieve, then no action is required.
- If you have NFS v4 only in your environment for archive or retrieve, then set the `_SHOWMOUNT_DISABLED` parameter to `TRUE` using the following steps:

  1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

     See Logging In to Oracle AVDF Appliances Through SSH.

  2. Switch to the `oracle` user.

     ```
     su - oracle
     ```

  3. Start SQL*Plus without the user name or password.

     ```
     sqlplus /nolog
     ```

  4. In SQL*Plus, run the following command:

     ```
     connect <super administrator>
     ```

  5. Enter the password when prompted.
  6. Run the following command:

     ```
     exec avsys.adm.add_config_param('_SHOWMOUNT_DISABLED','TRUE');
     ```

1. Log in to the primary Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Create new NFS locations by using the Audit Vault Server console.

   These new locations consider the newly mounted NFS points for both the primary and secondary Audit Vault Servers. Ensure that there is sufficient space in the newly created NFS locations to store all the necessary data files to be archived.

4. Start SQL*Plus without the user name or password.

   ```
   sqlplus /nolog
   ```

5. In SQL*Plus run the following command:

   ```
   connect super administrator
   ```

6. Enter the password when prompted.
7. Enable the archiving functionality by running the following command:

   ```
   exec management.ar.run_hailm_job('<NFS location name defined>');
   ```

   This command initiates a background job. You can view the status on the Jobs page. The name of the job is `HAILM POST UPGRADE JOB`.

   After you enable this functionality , all the archived data files are moved to the new NFS location and archiving is enabled after the job completes successfully.

7.2.6.8 Clear Unused Kernels from Oracle Audit Vault and Database Firewall

See My Oracle Support Doc ID 2458154.1 for instructions to clear unused kernels from Oracle Audit Vault and Database Firewall (Oracle AVDF).

7.2.6.9 Check the Observer Status After Updating to Oracle AVDF 20.7 or Later for High Availability

After upgrading from Oracle AVDF release 20.5 or 20.6 to release 20.7 or later in a high availability environment, you might encounter an issue with the Oracle Data Guard observer. The Audit Vault Server uses Oracle Data Guard to manage high availability.

To check the status of the Oracle Data Guard observer:

1. Log in to the standby Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Run the following commands:

```
dgmgrl /

show observer
```

The output displays the status and the last ping interval of the observers running on both primary and standby Audit Vault Servers. The last ping interval of both observers must have a specific duration in seconds.

4. If the output from the previous step doesn't display a specific duration for both observers, as shown in the following example, then complete the remaining steps to resolve the issue.

```
Host Name:                    <host name>
Last Ping to Primary:         (unknown)
Last Ping to Target:          (unknown)
```

a. Log in to the standby Audit Vault Server through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

b. Switch to the `oracle` user.

```
su - oracle
```

c. Run the following command:

```
/usr/local/dbfw/bin/observerctl --stop
```

d. Wait for one minute.

e. Run the following commands:

```
dgmgrl /

show observer
```

f. Verify that the last ping interval of both observers has a specific duration in seconds.

7.2.6.10 Configure Audit Vault Server Backups

The Audit Vault Server backup configuration file is release-specific and works on the same release for which it was created. Oracle recommends that you run the `avbackup config` command to create a new configuration file before performing the backup operation after updating Oracle Audit Vault and Database Firewall (Oracle AVDF).

7.2.6.11 Schedule Maintenance Jobs

Oracle Audit Vault and Database Firewall (Oracle AVDF) runs some jobs on the Audit Vault Server for proper and effective functioning of the system.

Oracle recommends that you run these jobs during a period when the Audit Vault Server usage is low, such as at night. You can schedule these jobs based on your time zone.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. In the **Configuration** section, click one of the following links, depending on your release:

Oracle AVDF Release	Link
20.1 and 20.2	**Manage**
20.3 and later	**Maintenance**

5. To schedule a new maintenance job, enter the start time in hours and minutes.

   The time that you specify here is the time on the browser.
6. In the **Time Out (In hours)** field, enter the duration of the maintenance job in hours.

   If the job doesn't complete in the specified duration, it times out.

> **Note:**
>
> The job runs at the specified start time daily. You can't change the repeat frequency.

7. Click **Save**.

7.2.6.12 Add a Privilege to the Native Network Encryption User for Decrypting the Native Network Encryption

If you're upgrading Audit Vault Server from release 12.2 to release 20 and a native network encryption user was already created on the target database for decrypting the native network encryption, you need to provide an additional privilege to the native network encryption user.

1. Log in to the target database as a user with administrative privileges.
2. Run the following command:

```
grant select on V_$SESSION to <NNE_USER>
```

   <NNE_USER> is the user that is configured in the target database for decrypting the native network encryption.

7.2.6.13 Retrieving the Security Assessment and Resetting the Baseline to a DBSAT 3.1 Assessment

After upgrading to Oracle AVDF 20.13, rerun the privilege script, retrieve the security assessment, and reset the baseline to one generated by DBSAT 3.1. This process ensures that the security posture of the environment is aligned with the latest assessment data, enabling more accurate monitoring and auditing of potential vulnerabilities.

See Confirm the Update Process for more information.

7.2.7 Recover the Database If an Update Fails

If you backed up Oracle Audit Vault and Database Firewall (Oracle AVDF) before updating, and if there is enough space in the Audit Vault Server's flash recovery area, you may be able to recover the database after a failed update under the guidance of Oracle Support.

To make recovery of the database possible, you should have the following amount of free space in the flash recovery area:

20 GB or 150% of the amount of data that is stored in the Audit Vault Server database, whichever is larger

For information on monitoring the flash recovery area, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

7.3 Patching Oracle AVDF 20.8 to Apply the Latest Release Update

To upgrade Oracle AVDF from release 12.2 to release 20.9 or later, first upgrade to release 20.8 and then apply the latest release update (RU) patch.

See Patching Oracle Audit Vault and Database Firewall Release 20 for instructions.

8

Uninstalling Oracle Audit Vault and Database Firewall

This chapter provides information on how to uninstall or remove Oracle Audit Vault and Database Firewall.

8.1 Uninstalling Audit Vault Agents Deployed on Target Host Machines

Uninstall the Audit Vault Server and the Database Firewall appliances, and the Audit Vault Agents, that are deployed on target host machines.

To remove the Audit Vault Agents from target host machines:

1. In the Audit Vault Server, stop all audit trails for the target host.
2. If the target host has Host Monitor Agent installed, uninstall it.
3. Verify the Audit Vault Agent is in `STOPPED` state.
4. In the Audit Vault Server, deactivate the Audit Vault Agent for the target host.
5. In the Audit Vault Server, delete the target host.
6. In the target host, delete the Audit Vault Agent install directory.

> **Note:**
>
> To uninstall the Audit Vault Server or Database Firewall, turn off the computers on which they are installed, and follow the procedures for safely decomissioning the hardware.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide*

8.2 Reimage Oracle Database Firewall and Restore from Audit Vault Server

About reimaging Oracle Database Firewall and restoring from Audit Vault Server.

Use this procedure to reimage the Oracle Database Firewall appliance and restore the configuration from the Audit Vault Server console.

1. Reinstall Database Firewall.

2. Configure the Database Firewall instance.

> **Note:**
>
> - Keep the same number of Network Interface Cards that were available in the previous instance and in the same order. However, there is no need to configure them manually except the Management Interface which is configured during installation. This task is accomplished by the reset Firewall operation.
> - Similarly, the proxy ports need not be created manually. This task is accomplished by the reset Firewall operation.
> - In case the Network Interface Cards or the proxy ports are created manually using the Audit Vault Server console, then the reset Firewall operation may not succeed and the state of the Firewall instance may not be same as before.
> - Do not execute `CONFIG-NIC` and `CONFIG-PROXY` commands to configure NIC and proxy ports.

3. Log in to the Audit Vault Server console as an administrator. Specify the Audit Vault Server certificate and IP address on the new Database Firewall instance.
4. Click on **Database Firewalls** tab. A list of Database Firewall instances configured are displayed on the main page.
5. The **Status** of the newly installed Database Firewall instance is `Down` with a red indicator. Click the name of the specific Database Firewall instance. The details of the specific Database Firewall instance is displayed on the main page.
6. Click **Update Certificate** button, and wait for the page to load. The status of the Database Firewall instance is `Up` or green.
7. Click **Reset Firewall** button. Confirm the operation by selecting **OK** in the dialog.
8. Check the status of this operation by navigating to the **Jobs** dialog. For this, click the **Settings** tab, and then click the **System** tab in the left navigation menu. Click the **Jobs** link under the **Monitoring** section.
9. The **Jobs** dialog contains a list of ongoing jobs. The Job Type is `Reset Firewall`. Click the **Job Details** page icon in the extreme left. The **Job Status Details** dialog contains current status. If the job has failed, then an appropriate message is displayed. If the job is successful, then it displays the completion time.
10. Check the overall health status of the Database Firewall instance. Navigate back to the **Database Firewalls** tab, and click on the specific instance. Click **Health Indicators** link, under **Diagnostics** section.
11. Expand the **Certificates** block. There is a message pertaining to certificate validation failure in the list, and take appropriate action.
12. Expand the **Database Firewall Monitoring** section and ensure everything is green. Click the **Close** button in the bottom right corner of the dialog.

A

Troubleshooting Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall provides troubleshooting advice for expected issues in the deployment or installation process.

A.1 Information to Provide Support When Filing a Service Request

Review this list of information to provide support when filing a service request.

> **Note:**
>
> Diagnostics data, especially trace files, often contains sensitive information. Protect it accordingly and only gather and send the information that's required.

- Oracle AVDF version, including any installed bundle patches
- If virtualization is being used? If so, which one?
- How much physical memory is available to Audit Vault Server and Database Firewall appliances?
- How much disk space was available with the initial installation?
- Did you add any SAN storage and in that case how much disk space?
- Provide any relevant details about the brand and model of the hardware being used. This is relevant if you have specific issues relating to booting from the installation media.
- Host OS for the secured target database and version, this is relevant for checking agent compatibility issues.
- Brand of the secured target database, such as Oracle, MySQL, SQL Server, etc.
- Version of the secured target database, including PSU and other one-off patches.
- Upload the alert.log file of the secured target database.
- From any Oracle secured target database provide the output of:
  - `show parameter audit`
  - `opatch lsinventory -patch -detail`
  - If unified auditing was configured (for some versions of Oracle database only)
  - Audit Trail type that is being configured and all relevant attributes
- Detailed diagnostic information for Audit Vault Server, see Downloading Detailed Diagnostics Reports for Oracle Audit Vault Server
- If requested by Oracle Support, diagnostic information from Oracle Trace File Analyzer. See Using Oracle Trace File Analyzer (TFA).

- Information about Database Firewall:
  - Detailed diagnostic info for Database Firewall, see Viewing the Status and Diagnostics Report for Database Firewall
  - How many Network Interface Cards are installed in the database firewall appliance?
  - Is the enforcement point using default password enumeration (DPE) or database activity monitoring (DAM)? If so is it bridge, span, or proxy?
  - Do you use VLAN tagging? There are restrictions for support of VLANs.
- For installation issues, diagnostic files related to the installation. See Collecting Logs to Debug Installation Failures.

Before contacting support, the Audit Trail Transaction Log should follow these guidelines:

- The user setup script must be run with the argument `REDO_COLL`
- The secured target database must be configured with `ARCHIVELOG`
- The streams recommended patches must be applied to the secured target db: Streams Recommended Patches (Doc ID 437838.1)
- `global_name` must be fully qualified (select global_name from global_name;)
- Parameter `global_names = true` is recommended
- If errors happen on capture or apply side please check respective alert.logfiles as you would do with any Streams related issue (av log will show only limited information for this audit trail type)

Related Topics

- Configure and Download the Diagnostics Report File

A.2 Error When Installing Audit Vault Server in Releases 20.1 to 20.3

Learn how to resolve an error observed when installing Audit Vault Server 20.1, 20.2, or 20.3.

Problem

An error is observed when installing Audit Vault Server. This is observed only in Oracle AVDF releases 20.1 to 20.3.

Solution

The Audit Vault Server installer (ISO) file is split into 3 parts or files in Oracle AVDF releases 20.1 to 20.3. All the three ISO files have to be concatenated to get a single Audit Vault Server 20.x ISO (`avdf-install.iso`) before proceeding with installation.

Refer to Downloading and Verifying Oracle AVDF Software for complete information.

Starting with Oracle AVDF 20.4, there is a single Audit Vault Server ISO file and there is no need to concatenate.

A.3 Conflicting Data on Storage Added to Oracle AVDF

Learn how to remove existing conflicting data from storage before adding it to Oracle Audit Vault and Database Firewall (Oracle AVDF).

Problem

The preexisting file system, Logical Volume Manager (LVM), or device mapper metadata may conflict with Oracle AVDF functionality. This may result in patch, upgrade, or installation failure.

Symptoms

The symptoms of any preexisting LVM or other device mapper metadata include, but are not limited to, the following:

- Two `vg_root` volume groups.
- Hard drive devices that become unavailable during patching, upgrade, or installation. This may lead to input or output errors and eventually result in patch, upgrade, or installation failure.

Solution

> **Caution:**
>
> This will erase data from the drive.

1. Download the latest Oracle Linux 8 ISO image from Oracle Linux Downloads.
2. Boot into rescue mode.
   a. Load the Oracle Linux 8 ISO onto your appliance and boot.

      The installation menu displays the following options:

      ```
      Install Oracle Linux 8.x.x
      Test this media & install Oracle Linux 8.x.x
      Troubleshooting
      ```

   b. Press the Down Arrow to select **Troubleshooting**, and press Enter.

      The troubleshooting menu displays the following options:

      ```
      Install Oracle Linux 8.x.x in basic graphics mode
      Rescue a Oracle Linux system
      ```

   c. Press the Down Arrow to select **Rescue a Oracle Linux system**, and press Enter.

      The rescue menu displays the following options:

      ```
      1) Continue
      2) Read-only mount
      3) Skip to shell
      4) Quit (Reboot)
      ```

   d. Type **3** (Skip to shell), and press Enter.

e. Press Enter again to open the shell prompt.

3. To discover the attached storage, enter the `lsblk` command at the shell prompt.

   For example:

```
sh-4.4# lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
loop0         7:0    0 745.4M  1 loop
loop1         7:1    0     4G  1 loop
├─live-rw   253:0    0     4G  0 dm   /
└─live-base 253:1    0     4G  1 dm
loop2         7:2    0    32G  0 loop
└─live-rw   253:0    0     4G  0 dm   /
sda           8:0    0   256G  0 disk
└─sda1        8:1    0   256G  0 part
sr0          11:0    1  11.2G  0 rom  /run/install/repo
sr1          11:1    1  1024M  0 rom
```

4. To wipe the drive, enter the `wipefs` command at the shell prompt.

   Enter `wipefs --help` to see a complete list of options.

   For example, to wipe the `/dev/sda` drive, enter the following command:

```
sh-4.4# wipefs --all /dev/sda
```

   The command output lists the changes. For example:

```
/dev/sda: 2 bytes were erased at offset 0x000001fe (dos): 55 aa
/dev/sda: calling ioctl to re-read partition table: Success
```

5. To safely power off, enter the `sync` command at the shell prompt, followed by `poweroff`.

```
sh-4.4# sync
sh-4.4# poweroff
```

6. After you wipe the drive, eject the ISO and restart the installation.

A.4 EFI Related Error When Installing Audit Vault Server on VMware

Learn how to resolve EFI related error when installing Audit Vault Server on VMware.

Problem

The following possible errors are observed when attempting to install Audit Vault Server on VMware:

```
EFI Virtual disk (0.0) … unsuccessful.
EFI VMware Virtual SATA CDROM Drive (0.0) … unsuccessful.
EFI Network …
```

Solution

There are important prerequisites to be followed while installing Audit Vault Server on VMware:

- You must set VMX configuration parameter *disk.EnableUUID* to `TRUE`. This must be done to enable proper mounting of disks. Without this setting, the Audit Vault Server installation on VMware will fail.
- You must set your virtual machine to use EFI boot. In some versions of VMware this is done by selecting the **VM Options** tab, then expanding **Boot Options**, and then choose `EFI` in the **Firmware** field. You must disable secure boot. Do not select the checkbox **Enable UEFI secure boot** field.

  This EFI boot setting is required only for fresh installation of Audit Vault Server specifically when the disk size is more than 2TB. This setting is not required for upgrade.

> **Note:**
>
> See Installing Audit Vault Server on VMware for complete information.

A.5 Cannot Access the Audit Vault Server Console

Learn the workaround for when you cannot access the Audit Vault server user interface or console.

Problem

The Audit Vault Server console is not accessible.

Solution

There are two remedies that you can perform depending on when this problem occurs:

- The problem occurs immediately after Audit Vault Server installation.

  In this case, the installation may not have been completed correctly. Perform the installation again.
- The problem occurs after the system is already running.

  In this case, check that the disk is not full and that the Oracle Audit Vault Server database is running using this command:

  ```
  /etc/init.d/dbfwdb status
  ```

  To restart the database, use run this command as `root`:

  ```
  /etc/init.d/dbfwdb start
  ```

  If you have a problem restarting the database, then contact Oracle Support.

A.6 Collecting Logs to Debug Installation Failures

You can collect logs to debug issues when installing Oracle Audit Vault and Database Firewall.

A.6.1 Collecting Logs for Base Operating System Installation Issues

Use these steps to collect logs for failures that happen during the installation of the base operating system (pre- or post-reboot).

Collecting logs for debugging pre-reboot installation failures

1. During installation or upgrade, after mounting the `.iso` file, press Tab to interrupt the normal boot process.
2. To collect logs, the installer must run with command line access. To enable command line access, remove the `noshell` from the boot option.
3. After the failure occurs, use one of the following keyboard shortcuts to access the command line:
   - Starting with Oracle AVDF 20.9 (Oracle Linux 8), press Ctrl+B and then press 2.
   - For installing Oracle AVDF 20.1 to 20.8 (Oracle Linux 7), press Alt+Right Arrow.
4. Run one of the following commands to start the collection tool:
   - Starting with Oracle AVDF 20.9 (Oracle Linux 8), use the following command:

     ```
     /usr/libexec/platform-python /run/install/repo/collect_diagnostics.py
     ```

     For Oracle AVDF 20.1 to 20.8 (Oracle Linux 7), use the following command:

     ```
     python /run/install/repo/collect_diagnostics.py
     ```
5. Follow the instructions to collect the diagnostics file.

Collecting logs for debugging post-reboot installation failures

1. Using the password you have previously set, log in as `root` on the console or using SSH.
2. Run one of the following commands to start the collection tool:
   - Starting with Oracle AVDF 20.9 (Oracle Linux 8), use the following command:

     ```
     /usr/libexec/platform-python /media/avdf-install/collect_diagnostics.py
     ```
   - For Oracle AVDF 20.1 to 20.8 (Oracle Linux 7), use the following command:

     ```
     python /media/avdf-install/collect_diagnostics.py
     ```
3. Follow the instructions to collect the diagnostics file.

Transferring the log file for analysis

After following the instructions to collect the logs for pre- or post-reboot failures, the collection tool should have created a log or diagnostic file in the following location:

```
/root/install-diagnostics.tgz
```

1. Follow the instructions at the prompt to transfer the log file for analysis. Use the following command:

   ```
   scp /root/install-diagnostics.tgz <user>@<Ip address>:<Path>
   ```

2. You may also perform the following steps and commands to configure the network:

   ```
   ip addr add <IP address>/<sub net> dev <interface>
   ```

   ```
   ip link set <interface> up
   ```

   ```
   ip route add default via <gateway>
   ```

3. Use the information available in the log file to analyze the issue and then try the installation again after addressing the issue.

A.6.2 Collecting Logs for Oracle AVDF Installation Issues

Use these steps to collect logs for failures that happen when installing Oracle AVDF.

1. At the install start screen, press Tab (and delete the word "noshell").
2. Press Enter to begin the installation.
3. After the installation begins, press Ctrl+B and then press 2.

   The login screen should appear even if the installation fails.
4. Use tar or Gzip to collect the following logs:
   - `/var/log`
   - `/var/lib/oracle/diag`
   - `/var/lib/oracle/oraInventory/logs`
   - `/tmp`
5. Collect the following configuration files:
   - `/etc/sysconfig/avdf`
   - `/var/lib/avdf/system_history.yaml`
   - `/usr/local/dbfw/etc/dbfw.conf`
6. Collect the output from the following commands:
   a. `su root`
   b. `rpm -qa avs`
   c. `ls -lrt /var/log/installation-*`
   d. `ls -lrt /var/log/upgrade-*`
   e. `df -h`
   f. `du -sh /var/lib/oracle/19.7.0.0.0`
   g. `du -sh /var/lib/oracle/19.7.0.0.0/grid`
   h. `cat /proc/meminfo`

7. Collect the output from the following commands:
   a. `su root`
   b. `hostname`
   c. `cd /var/lib/oracle/diag`
   d. `ls -lrt`
   e. `cd crs`
   f. `ls -lrt`
   g. `hostname`
   h. `cd <hostname>`
   i. `ls -lrt`
   j. `cd crs`
   k. `ls -lrt`

A.7 Unable to Reach Gateway Error

Learn to fix incorrect Gateway details entered during installation.

Problem

Incorrect or invalid Gateway details entered while installing Audit Vault Sever or Database Firewall. The following error message may be encountered:

```
Gateway is not reachable from host
```

Solution

The Gateway details can to be corrected by following these steps:

1. Log in to **Terminal-1** as *root* user. Alternately, **Terminal-1** can be accessed by pressing `Ctrl+Alt+Right Arrow Key`.
2. Access and open the dbfw.conf file by executing this command:

   ```
   vi /usr/local/dbfw/etc/dbfw.conf
   ```

3. Set the correct value for the **GATEWAY** field by overwriting the existing value.
4. Save and close the file.
5. Execute the command to apply the modified value:

   ```
   /usr/local/dbfw/bin/priv/configure-networking
   ```

6. Return back to the appliance screen by pressing `Ctrl+Alt+Left Arrow Key`.

> **Note:**
>
> The network settings entered during installation can be modified, by choosing the **Change IP Settings** option in the installer or appliance screen.

A.8 Issue with Configuring or Managing Oracle AVDF through Oracle Enterprise Manager Cloud Control

Learn how to solve an issue with configuring or managing Oracle AVDF through Oracle Enterprise Manager Cloud Control.

Problem

Unable to configure or manage Oracle AVDF through Oracle Enterprise Manager Cloud Control.

Solution

Oracle AVDF plug-in is an interface within Oracle Enterprise Manager Cloud Control for administrators to manage and monitor Oracle AVDF components. Refer to System Monitoring Plug-in User's Guide for Audit Vault and Database Firewall in case of any issues when configuring the Oracle EM plug-in.

Refer to Compatibility with Oracle Enterprise Manager to check the supported versions of Oracle Enterprise Manager with Oracle AVDF 20.

A.9 Installation Stops Progressing After Entering the IP Address

Learn what to do when the installation stops progressing.

Problem

When installing Audit Vault Server, the installation stops progressing after you enter the IP address.

Solution

1. Follow the instructions in Collecting Logs for Oracle AVDF Installation Issues to debug and collect logs for Oracle AVDF 20 installation issues.
2. File a service request (SR) and attach the collected diagnostic information to the SR.

A.10 No Signal Error During Post-Install Tasks

Learn what to do when you receive a "no signal" error.

Problem

During the installation you receive a "no signal" error with a green screen, and the installation takes a long time to complete.

Solution

1. Capture the screen content.
2. Follow the instructions at Collecting Logs for ORacle AVDF Installation Issues to debug and collect logs for Oracle AVDF 20 installation issues.
3. File a service request (SR) and attach the screen capture and the collected diagnostic information to the SR.

A.11 Pre-upgrade RPM Warnings

While patching or upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), the pre-upgrade RPM displays warnings to indicate issues that you need to resolve before proceeding with the update.

A.11.1 RPM Upgrade Failed

Read the troubleshooting advice if RPM upgrades fail.

Problem

An RPM upgrade failed with the following error:

```
error: %post(dbfw-mgmtsvr-###) scriptlet failed, exit status 1
```

Solution

1. Check that there is at least 10MB of free `/tmp` space.
2. Remove the new RPM:

   ```
   rpm -e dbfw-mgmtsvr-###
   ```
3. Retry the upgrade.

A.11.2 Uninstalling the Pre-Upgrade RPM for AVDF 20.12 and Later Doesn't Remove Filesystem

If you currently have Oracle AVDF 20.11 or earlier and apply the pre-upgrade RPM for AVDF 20.12 or later, and decide to not proceed with the upgrade, the filesystem for Database Firewall doesn't get removed. If you wish to reallocate the space reserved for upgrade, perform the following.

1. Run the following command to find the exact version of the pre-upgrade RPM:

   ```
   rpm -q avdf-pre-upgrade
   ```
2. Run the following command to uninstall and remove the pre-upgrade RPM:

   ```
   rpm -e {rpm name}
   ```
3. Run the following command to verify the filesystem remains mounted:

   ```
   # df
   ```

   You will see something similar to:

   ```
   [...]
   /dev/mapper/vg_root-lv_var_dbfw_upgrade on /var/dbfw/upgrade type
   ext4(rw,relatime,seclabel)
   [...]
   ```

4. Run the following command to unmount the filesystem:

```
umount /var/dbfw/upgrade
```

5. Run the following command to remove the logical volume:

```
lvremove /dev/vg_root/lv_var_dbfw_upgrade
```

6. Run the following command to confirm the logical volume is unmounted and removed:

```
# df
# lvs
```

You will see something similar to:

```
[no /var/dbfw/upgrade records]
[no /var/dbfw/upgrade records]
```

A.11.3 Pre-upgrade RPM Failure Due to Insufficient Memory

Learn how to resolve pre-upgrade RPM failure due to insufficient memory.

Problem

Installing the pre-upgrade RPM places the system in a safe state, performs multiple checks, and rearranges free space on the appliance for a safe and successful installation or upgrade of Audit Vault Server and Database Firewall.

The following error may be observed:

```
AVDF::Installer::Upgrade::InvalidPreconditions
Recommended memory is x.yy GB; system only has xx.yy MB available
ERROR:
AVDF::Installer::Upgrade::InvalidPreconditions
Verifying pre-upgrade conditions failed.
```

Solution

Follow these steps to resolve this issue:

1. Run the following command to find the exact version of the pre-upgrade RPM:

```
rpm -q avdf-pre-upgrade
```

2. Run the following command to uninstall and remove the pre-upgrade RPM:

```
rpm -e {rpm name}
```

3. Power off the host machine.
4. Increase the memory as per the recommendation.
5. Power on the host machine.
6. Re-install the pre-upgrade RPM.

7. Ensure to check the warnings related to memory are resolved.
8. Proceed with the upgrade as per Oracle AVDF documentation.

A.11.4 Insufficient Space Error in /var/lib/oracle File System Reported by Pre-upgrade RPM

Learn how to fix insufficient space error issue in `/var/lib/oracle (lv_oracle)` file system reported by pre-upgrade RPM.

Problem

An error or issue is observed when running pre-upgrade RPM. There is insufficient space in `/var/lib/oracle (lv_oracle)` file system.

Solution

The `/var/lib/oracle` file system needs a minimum of 31 GB free space for performing upgrade.

Follow these steps to clear space in `/var/lib/oracle` and to proceed with the upgrade process:

1. Run the following command as *grid* user:

   ```
   /usr/bin/find /var/lib/oracle/grid/rdbms/audit -name '*.aud' -mtime +1 -
   delete
   ```

   This process may take up to one hour to complete.
2. Create another terminal.
3. Run the following command as *grid* user to remove the `trc` and `trm` files:

   ```
   rm /var/lib/oracle/diag/asm/+asm/+ASM/trace/*.tr[cm]
   ```

4. As *root* user check if the `/var/lib/oracle/upgrade_iso_file` directory exists. Remove the ISO file in case it exists.
5. As *root* user check and remove these file in case they exist.

   ```
   rm /var/lib/oracle/software/database.tar.xz
   ```

   ```
   rm /var/lib/oracle/dbfw/av/grid[12].zip
   ```

6. Run the following command as *oracle* user and remove the `trc` and `trm` files:

   ```
   rm /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb/trace/*.tr[cm]
   ```

7. Clear diagnostic logs through the Audit Vault Server console. This process may also release some additional space. In case any of the components are set to `Debug`, then set them to `Warning`.

> **Note:**
>
> Clearing Diagnostic Logs

A.11.5 Insufficient Space Error in / File System Reported by Pre-upgrade RPM

Learn how to fix insufficient space error issue in the / file system reported by pre-upgrade RPM.

Problem

An error similar to the below message is observed when running pre-upgrade RPM. There is insufficient space in the / file system.

```
Checking upgrade preconditions
This upgrade requires at least 2.35GiB free on / (actual: 2.29GiB)

    AVDF::Installer::Upgrade::InvalidPreconditions

Precondition: 'space-check.rb'
    Result: 'Please follow the instructions in the Administrator's Guide to
add storage, then retry.
    Summary: AVDF::Installer::Upgrade::InvalidPreconditions
        System is not ready for upgrade.
```

Solution

Extend / using the free space from vg_root:

```
lvextend --resizefs -L+2.35G /dev/vg_root/lv_ol8root
```

A.11.6 Pre-upgrade RPM Could Not Stop Certain Processes During Oracle AVDF Upgrade

Learn how to fix warnings or errors pointed by pre-upgrade RPM while upgrading Oracle AVDF.

Problem

The pre-upgrade RPM performs necessary checks to prepare the appliance conducive for upgrade. It stops certain processes running on the appliance in due course. In some cases, some of the processes cannot be stopped by the pre-upgrade RPM. It results in the following errors or warnings:

```
Not all processes were stopped


target is busy
```

Solution

Follow these steps:

1. The pre-upgrade RPM suggests a possible way or solution to figure out the specific processes that are still running. Follow the instructions and stop the specific processes.
2. Uninstall the pre-upgrade RPM.
3. Reinstall the pre-upgrade RPM.
4. Proceed with the upgrade procedure.

A.11.7 Pre-upgrade RPM Fails with "Unable to Stop Observer"

Learn how to resolve the "unable to stop observer" warning in the pre-upgrade RPM.

Problem

The pre-upgrade RPM fails with the "unable to stop observer" warning.

Messages and debug files display one of the following errors when the observer was started:

`'DGMGRL:ORA-28000: The account is locked.'` or `'DGMGRL:ORA-28001: the password has expired'`

Solution

This can happen if the `sys` password has expired or the `sys` user is locked. To resolve this issue, update the `sys` user on the primary and standby systems. See Verify That the SYS User Is Unlocked and the Password Is Not Expired for instructions.

A.11.8 Pre-upgrade RPM Check: Alert Queue Space Warning

The pre-upgrade RPM displays a warning if the system doesn't have sufficient space to purge the alert queue during the upgrade.

The following warning appears:

```
The system does not have sufficient space to purge alert queue. Refer to Installation Guide on how to resolve this.
```

To resolve this issue, see Ensure That the System Has Sufficient Space to Purge the Alert Queue for instructions.

A.11.9 Pre-upgrade RPM Check: Boot Device Is Greater Than 2 TB

The pre-upgrade RPM warns you if the boot device greater than 2 TB, in which case the upgrade process may fail. Ensure that the boot device is less than 2 TB before upgrading.

To resolve this issue, see Ensure That the Boot Device Is Less Than 2 TB for instructions.

A.11.10 Pre-upgrade RPM Check: Boot Partition Space Warning

The pre-upgrade RPM warns you if there is not enough space in the boot partition, in which case the upgrade process may fail. Ensure that the boot partition has at least 500 MB before upgrading.

To resolve this issue, see Ensure That the Boot Partition Has at Least 500 MB for instructions.

A.11.11 Pre-upgrade RPM Check: Legacy Crypto Warning

If your current Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 deployment has Host Monitor Agents or Audit Vault Agents on AIX and you're upgrading to Oracle AVDF 20.4 or later, then the pre-upgrade RPM displays a warning about TLS and encryption.

To resolve this issue, you need to run commands both before and after the upgrade.

Upgrading from Oracle AVDF 12.2.0.11.0 and Earlier

When upgrading from Oracle AVDF 12.2.0.11.0 and earlier, the pre-upgrade RPM displays the following warning. Follow the instructions in the warning to resolve the issue.

```
If you have deployed Host Monitor Agents (or Audit Vault Agents on AIX) in your
environment, TLS 1.1 should be used for encryption instead of the default version
of TLS 1.2. Else, Host Monitor Agents (or Audit Vault Agents on AIX) will not
upgrade automatically. If you wish to use TLS 1.1 for encryption run the below
command before proceeding with the upgrade.

ruby /usr/local/dbfw/bin/upgrade/configure_tls_settings.rb 2


Post Audit Vault Server and Agents upgrade, run the following command as root
user:

/usr/local/dbfw/bin/priv/configure-networking --agent-tls-cipher-level 4


Run the following command post upgrade, if it is only displayed on the prompt:

/usr/local/dbfw/bin/priv/send_agent_update_signal.sh


Refer to Oracle AVDF Installation Guide, sections "Pre-upgrade RPM Legacy Crypto
Check Warning" and "Post Upgrade TLS Security Hardening" for more details.
```

Upgrading from Oracle AVDF 12.2.0.12.0 and Later

When upgrading from Oracle AVDF 12.2.0.12.0 and later, the pre-upgrade RPM displays the following warning. Follow the instructions in the warning to resolve the issue.

```
If you have deployed Audit Vault Agents on AIX in your environment, TLS 1.1
should be used for encryption instead of the default version of TLS 1.2. Else,
the Agents on AIX will not upgrade automatically. If you wish to use TLS 1.1 for
encryption run the below command before proceeding with the upgrade.

ruby /usr/local/dbfw/bin/upgrade/configure_tls_settings.rb 2


Post Audit Vault Server and Agents upgrade, run the following command as root
user:

/usr/local/dbfw/bin/priv/configure-networking --agent-tls-cipher-level 4
```

```
Run the following command post upgrade, if it is only displayed on the prompt:

/usr/local/dbfw/bin/priv/send_agent_update_signal.sh

Refer to Oracle AVDF Installation Guide, sections "Pre-upgrade RPM Legacy Crypto
Check Warning" and "Post Upgrade TLS Security Hardening" for more details.
```

Related Topics

- Set the Host Monitor Agent and Audit Vault Agent TLS Version
  If your current Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 deployment has Host Monitor Agents or Audit Vault Agents on AIX and you're upgrading to Oracle AVDF 20.4 or later, set the TLS version to TLS 1.1 before upgrading.
- Post Upgrade TLS Security Hardening
  If your previous Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 deployment had Host Monitor Agents or Audit Vault Agents on AIX and you upgraded to Oracle AVDF 20.4 or later, then you set the TLS version to TLS 1.1 before upgrading. After upgrading, you should reset the TLS level.

A.11.12 Pre-upgrade RPM Fails with "Not All Processes Were Stopped"

Problem

The pre-upgrade RPM fails with the following warning: `Not all processes were stopped: 7378,7379`.

For example:

```
rpm -ivh --force avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
Preparing... ########################################### [100%]
1:avdf-pre-upgrade ########################################### [100%]
Checking upgrade preconditions
/bin/df: '/var/dbfw/upgrade': No such file or directory
/bin/df: no file systems processed
Shutting down services.
Traceback (most recent call last):
3: from /usr/local/dbfw/bin/pre_upgrade.rb:642:in '<main>'
2: from /usr/local/dbfw/bin/pre_upgrade.rb:614:in 'process_command_line'
1: from /usr/local/dbfw/bin/pre_upgrade.rb:503:in 'post_install'
/usr/local/dbfw/lib/ruby/upgrade/common.rb:621:in 'stop_nonroot_processes':
Not all processes were stopped: 7378,7379
```

Cause

This issue could be caused by an idle SSH session, busy devices, or open temporary files.

Solution

1. Uninstall the RPM as the `root` user.
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.
      See Logging In to Oracle AVDF Appliances Through SSH.

b. Uninstall the pre-upgrade RPM by using one of the following commands:

```
rpm -e avdf-pre-upgrade


rpm -e avdf-pre-upgrade --noscripts
```

2. Check the pre-upgrade RPM listing.
   a. Enter the following command:

```
rpm -qa |grep avdf-pre-upgrade
```

   b. Ensure that there's no entry for `avdf-pre-upgrade` RPM.
   c. Reboot the Audit Vault Server if it's a `STANDALONE` system.
3. Check for other SSH sessions, busy devices, or temporary open files.
   a. Ensure that there are no other SSH sessions that are owned by the `support` user.

      To do this, identify idle notty (no tty) SSH sessions and try to stop them.

      Use the following commands to check the `pid` of `sshd: support@notty`.

```
ps -ef |grep support


ps -ef |grep notty
```

      For example:

```
support 2480 2427 0 18:31 ? 00:00:00 sshd: support@notty
support 2481 2480 0 18:31 ? 00:00:00 -bash
kill -9 2481
kill -9 2480
```

   b. Check again for `support@notty` processes in the system.
   c. Ensure that the system doesn't have any busy devices or open temporary files. To do this, run `lsof` against `/tmp` and `/usr/local/dbfw/tmp`.

      For example:

```
lsof /usr/local/dbfw/tmp
lsof /tmp
```

> **Note:**
>
> Ensure that no logs are open when starting the patching or upgrade process.

4. Try to install the pre-upgrade RPM as the `root` user.
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

b. Enter the following command:

```
rpm -i /root/avdf-pre-upgrade-20.x.0.0.0-0_NNNNNN.NNNN.x86_64.rpm
```

A.11.13 Pre-upgrade RPM Check: Agent Failure Checks - Upgrade Prerequisites

Starting with Oracle AVDF 20.9, the pre-upgrade RPM verifies that the Audit Vault Agent and Host Monitor Agent configurations are compatible with Oracle AVDF 20.10 or later.

Problem

The `agent_prereq_checks_failure_report.txt` report indicates that a Audit Vault Agent or Host Monitor Agent doesn't meet the prerequisites to update to Oracle AVDF 20.10 or later. You can find the agent success and failure reports in the following locations:

- Success report: `/opt/avdf/report/agent_prereq_checks_success_report.txt`
- Failure report: `/opt/avdf/report/agent_prereq_checks_failure_report.txt`

The following example shows a failure message:

```
Agent/HM Validation Failure statuses are as below :
-------------------------------------------------------------------
Agent Name : agent-linux
Agent Validation Status : FAILURE
Agent Failure Checks : Upgrade Prerequisites check jar build with latest
version. Please check the minimum java version required. - <Exception Message>
Agent Checks Warning Messages :
Validated at : 2022-12-02 09:11:24.774880
```

Solution

Resolve the issue that's indicated in the report. For example, update the Audit Vault Agent machine to the minimum Java version that's supported.

You can rerun the failure check scripts individually to verify that the issues are resolved. Run these scripts as the `root` user.

```
/usr/bin/python3 /usr/local/dbfw/bin/upgrade/pre_upgrade_validate_agent.py
standalone
```

```
/usr/bin/python3 /usr/local/dbfw/bin/upgrade/
pre_upgrade_download_agent_validation_status.py standalone
```

A.12 SSH Becomes Disabled After Updating Oracle AVDF with FIPS Enabled

If SSH becomes disabled after updating Oracle AVDF with FIPS mode enabled, update the SSH keys to be compliant with FIPS.

Problem

After updating Oracle AVDF to release 20.9 with FIPS mode enabled, SSH becomes disabled.

Solution

Before enabling FIPS 140-2, ensure that your SSH keys are compliant with FIPS. If your SSH keys are not compliant with FIPS, the SSH connection with the appliance might be lost after enabling FIPS.

For Oracle AVDF on Oracle Cloud Infrastructure (OCI), before enabling FIPS mode, ensure that the `opc` user has FIPS-compliant keys registered to `/home/opc/.ssh/authorized_keys`.

Follow these steps to resolve this issue:

1. Log into the Audit Vault Server console and disable FIPS mode.
2. Log back into the appliance through SSH and check or update the user keys for SSH-enabled users in `~/.ssh/authorized_keys` to be compliant with FIPS.

   It can take several minutes for the console to become available after enabling or disabling FIPS mode.
3. Enable FIPS mode.

Related Topics

- Enabling FIPS 140-2 on the Audit Vault Server

A.13 SSH Connection Times Out When Uninstalling the Pre-Upgrade RPM

Problem

The SSH connection times out when uninstalling the pre-upgrade RPM.

Cause

The default SSH connection timeout is 10 minutes, and uninstalling the pre-upgrade RPM can take longer than 10 minutes.

Solution

Run the `screen` command before uninstalling the pre-upgrade RPM. The `screen` command prevents network disconnections from interrupting the patching or upgrading.

If the session terminates, resume by switching to the `root` user and then running the `screen -r` command.

A.14 Installation Pauses After Entering the Root Password

Problem

When you start the installer for Oracle AVDF 20.5, it installs a few packages and prompts you to change the root password. After you enter the new root password, the installer immediately display some unmount commands and returns to the starting installation screen. You're unable to proceed with the installation.

Cause

The ISO file was removed before the installation was completed.

Solution

After you enter the new root password and return to the starting installation screen, complete the following steps:

- Remove the ISO CD from the CD drive and restart the machine.
- When you're promoted to log in, log in as `ROOT`.
- When promoted for the ISO file, add the ISO file from the media.

A.15 When Upgrading to Oracle AVDF 20.3 `ELMIG_POPULATE_CLUSTERS_202` and `ELMIG_CONVERT_HASH_202` Are Reported as `INVALID` in `dba_objects` Table

Even though the objects are invalid this doesn't have any impact on the system operation and can be ignored.

Problem

When upgrading to Oracle AVDF 20.3 the objects `ELMIG_POPULATE_CLUSTERS_202` and `ELMIG_CONVERT_HASH_202` are reported as `INVALID` in `dba_objects` table.

The following query results in the `ELMIG_POPULATE_CLUSTERS_202` and `ELMIG_CONVERT_HASH_202` objects.

```
elect object_name from dba_objects where status = 'INVALID';
OBJECT_NAME
```

Solution

This doesn't have any impact on the system operation and can be ignored.

A.16 Error Occurred Trying to Format `SDAF1` When Installing Oracle AVDF

Problem

During the installation of Audit Vault Server,the following error is encountered:

```
Error: An error occurred trying to format sdaf1. This problem is serious, and the
install cannot continue. Press to reboot your system.
```

Cause

The server has SAN connectivity.

Solution

Disable the SAN connectivity. ISCSI device should not be attached until Audit Vault Server installation is completed.

A.17 Audit Vault Agent Failed on Startup: `OAV-10: Failed to Release Connection to DB`

Problem

When installing the Audit Vault Agent error `OAV-10: Failed to Release Connection to Database` occurred when `./agentctl start -k` was executed. The database to Audit Vault Server connection failed.

Cause

The wrong location was used for `JAVA_HOME` and `agentctl` picked up a different Java in the path. The connection failed as it does not work with Java that is present in the database home.

Solution

Set the proper location for `JAVA_HOME`:

```
JAVA_HOME=/usr/java/jdk1.8.0_361
export PATH=$JAVA_HOME/bin:$PATH
```

A.18 Upgrade to AVDF 20.4 Failed During `upgrade_apex` Step

When upgrading to AVDF 20.4, the `upgrade_apex` step results in `ODF-10001: Internal error: FAILED migration: upgrade_apex (as oracle)` error.

Problem

The `/var/log/messages` contains `ERROR - ODF-10001: Internal error: FAILED migration: upgrade_apex (as oracle) (applied change)` and `/var/log/debug` contains

```
upgrade_apex: error: cannot create /var/lib/oracle/dbfw/apex/images/
computer.gif
upgrade_apex: Permission denied
upgrade_apex: error: cannot create /var/lib/oracle/dbfw/apex/images/
phone_support.gif
upgrade_apex: Permission denied
```

In addition, running the following command as the `root` user:

```
/opt/avdf/bin/privmigutl -status
```

results in

```
System state - recovery
Migration set 'AVS' - failed
Last migration 'Upgrading apex20' - failed
```

Solution

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run the following command:

   ```
   chown -R oracle:oinstall /var/lib/oracle/dbfw/apex/images
   ```
3. Switch to the `oracle` user.

   ```
   su - oracle
   ```
4. Run the following script:

   ```
   /usr/local/dbfw/etc/privileged-migrations/upgrade_apex
   ```
5. Run

   ```
   echo $?
   ```

   If the result is 2, then the script has completed successfully.
6. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
7. Resume the upgrade process by running the following:

   ```
   /opt/avdf/bin/privmigutl --resume --confirm
   ```

   Make the sure ssh connection to the Oracle AVDF server is reliable and does not terminate while running this command.
8. Check if the `$ORACLE_HOME/apex/images` folder and its contents have `oracle:oinstall` permission, and if not, grant these permissions.

Related Topics

- Patching Oracle Audit Vault and Database Firewall Release 20

A.19 Missing "Save as" Option in Web Console After Upgrading Oracle Audit Vault Server

Problem

After upgrading the Audit Vault Server from Oracle AVDF 12.x to 20.x, the "Save As" option is no longer available in the UI Web Console on certain pages. Previously, this option was used to save pages from the **Audit Trail Table Listing** and **Host Table Listing**, now making it difficult for users to generate reports in newer versions.

Cause

Customers rely on the "Save As" option to create reports from the **Audit Trail** and **Host Table Listings** for audit reviews and management presentations. The new UI in versions 20.1 to 20.4 removed this option, causing a disruption in existing workflows for auditors.

Solution

To work around the missing "Save As" feature, users can manually run SQL queries to extract the necessary data. These queries can then be formatted into HTML or PDF reports using SQL developer, SQL*Plus, or other tools.

Example Queries:

- **Audit Trail Query:** This query can be used to get a table as seen on the Audit Trail page.

```
Select
st.secured_target_name,atv.location,atv.audit_trail_type,atv.host_name,atv.
status,stt.secured_target_type_name,atv.error_message,atv.collection_autost
art,atv.trail_autostart_attempts,atv.trail_last_start_time,
(select checkpoint_time from avsys.checkpoint c
where c.audit_Trail_id = atv.audit_Trail_id )Last_Collection_Time
from avsys.audit_trail_view atv, avsys.secured_target
st,avsys.secured_target_type stt
where atv.source_id = st.secured_target_id and st.secured_target_type_id =
stt.secured_target_type_id and st.active = 'Y' and atv.active ='Y';
```

- **Host Page Data Query:** This query can be used to get table as seen on Host page.

```
select a.host_name, a.host_ip, a.activation_key, upper(a.status) as
agent_status, a.activation_time,
a.platform, a.agent_location, a.version, h.HOSTMON_INSTALL_STATE,
h.HOSTMON_LOCATION,
h.HOSTMON_VERSION, h.HOSTMON_ZIP_GEN_TIMESTAMP,
h.HOSTMON_UPDATE_TIMESTAMP, h.AGENT_OS_USER,
h.HOSTMON_ERROR_MSG, hs.STATUS_TIMESTAMP as last_connected_At
from avsys.agent_view a, avsys.hostmon_view h, avsys.host hs
where a.host_ip = h.host_ip and hs.host_ip = h.host_ip and hs.host_ip =
a.host_ip
and a.deleted_at is null and h.deleted_at is null and hs.deleted_at is
null;
```

- Generating HTML Reports: Users can follow these steps to generate presentable HTML reports using SQL*Plus:

```
set LINESIZE 4000; set PAGESIZE 4000; column SECURED_TARGET_NAME format
a20; column
      TRAIL_AUTOSTART_ATTEMPTS format 9; column AUDIT_TRAIL_TYPE format
a10; column host_name format
      a25; column status format a12; column TRAIL_AUTOSTART_ATTEMPTS
format 9; column location
      format a32; column TRAIL_LAST_START_TIME format a30; column
LAST_COLLECTION_TIME format a30;
      column ERROR_MESSAGE format a80; set colsep '|'

Select
st.secured_target_name,atv.location,atv.audit_trail_type,atv.host_name,atv.
status,stt.secured_target_type_name,
atv.error_message,atv.collection_autostart,atv.trail_autostart_attempts,atv
.trail_last_start_time,
(select checkpoint_time from avsys.checkpoint c where c.audit_Trail_id =
atv.audit_Trail_id )
Last_Collection_Time from avsys.audit_trail_view atv, avsys.secured_target
st,
avsys.secured_target_type stt where atv.source_id = st.secured_target_id
and
st.secured_target_type_id = stt.secured_target_type_id and st.active = 'Y'
and atv.active ='Y';
```

Execute the following query to generate the report:

```
SET ECHO OFF
SET PAGESIZE 4000
SET FEEDBACK OFF
SET TERMOUT OFF
SET MARKUP HTML ON TABLE ""
SPOOL AuditTrail.html

Select
st.secured_target_name,atv.location,atv.audit_trail_type,atv.host_name,atv.
status,stt.secured_target_type_name,

atv.error_message,atv.collection_autostart,atv.trail_autostart_attempts,atv
.trail_last_start_time,
      (select checkpoint_time from avsys.checkpoint c where
c.audit_Trail_id = atv.audit_Trail_id )
      Last_Collection_Time from avsys.audit_trail_view atv,
avsys.secured_target st,
      avsys.secured_target_type stt where atv.source_id =
st.secured_target_id and
      st.secured_target_type_id = stt.secured_target_type_id and st.active
= 'Y' and atv.active =
      'Y'; SPOOL OFF
```

A.20 Oracle AVDF 20.7 Installation Fails Due to Package Download Error

While installing Oracle AVDF 20.7, the installation failed to complete the Oracle Audit Server Installation.

Problem

The installation of Oracle AVDF 20.7 installation fails with the error:

```
Installation failed: Failed to complete the Oracle Audit Server Installation
```

Cause

The following error appears in the debug logs, indicating an issue with package downloads:

```
localhost run-privileged-migrations[22598]:
com.oracle.dbfw.privilegedMigration DEBUG - yum: Error downloading packages:
localhost run-privileged-migrations[22598]:
com.oracle.dbfw.privilegedMigration DEBUG - yum:
avs-grid-<version>.x86_64: [Errno 256] No more mirrors to try.
```

This occurs when the installation ISO is unavailable during part of the installation or if network issues interrupt the download process.

Solution

To resolve the issue, follow these steps:

1. Verify the ISO file:
   a. Ensure the ISO file is completely downloaded and accessible throughout the installation.
   b. Verify the download by checking the file size and comparing the SHA-256 checksum. Run the following command on Linux to generate the checksum:

      ```
      $ sha256sum Vpart_number.iso
      ```

   c. Confirm the checksum matches the value provided in the File Download dialog box.
2. Check ISO Accessibility:
   a. After mounting the ISO to the Audit Vault Server (AVS) as root, confirm it is recognized by the system:

      ```
      ls /dev/disk/by-label
      ```

      Look for a label like `AVS_20_7_0_0_0`.
   b. Mount the ISO with:

      ```
      mount /dev/disk/by-label/AVS_20_7_0_0_0 /mnt
      ```

c. Verify that the required package files are present:

```
find /mnt -name 'avs-grid*' -ls
```

3. Network Stability Check:

a. From the AV server, test the network stability with:

```
cat 'Copy one of the files from find /mnt -name "avs-grid*" -ls' > /dev/
null
```

b. If this command is slow, network slowness may be affecting the installation. Check `/var/log/messages` for additional error logs.

If any issue persist, re-download the ISO file and confirm checksum accuracy before retrying the installation.

> **Note:**
>
> This issue has also been observed in Oracle AVDF version 20.8.

A.21 Calculating Minimum Required In-Memory Size for AVDF to Prevent "Insufficient Memory" Errors

Learn how to find sufficient memory to populate tables to In-Memory area if you receive an "insufficient memory" error.

Problem

The AVDF system may display an "Insufficient memory" error if adequate memory is not allocated to the In-Memory area for storing `EVENT_LOG` data.

Solution

To calculate the minimum required memory in bytes for storing `EVENT_LOG` data in In-Memory for a one-month period, follow these steps:

1. Run the Primary Query
Execute the following SQL query to determine the required memory allocation:

```
SELECT NVL(MAX((SUM(msize)) / (SELECT EXTRACT(DAY FROM (partition_end -
partition_start))
FROM avsys.dw_partition_view WHERE partition_name=pname)), 0)
FROM (SELECT s.partition_name pname, (i.inmemory_size +
i.bytes_not_populated) msize
      FROM user_tab_subpartitions s, v$im_user_segments i
      WHERE s.subpartition_name=i.partition_name
      AND s.table_name='EVENT_LOG'
      AND i.segment_name='EVENT_LOG')
GROUP BY pname;
```

2. Calculate the Required Memory

- Multiply the output of the above query by `31*1.2` (for a maximum of 31 days in a month and an additional 20% buffer for days with more data).
- The resulting value is the minimum required memory in bytes for one month.

3. Alternative Calculation (if the query returns 0)
   If the primary query returns 0, run this alternative query to estimate the required memory:

```
SELECT MAX((SUM(r.bytes)) / (SELECT EXTRACT(DAY FROM (partition_end -
partition_start))
FROM avsys.dw_partition_view WHERE partition_name=pname))
FROM (SELECT s.partition_name pname, u.bytes
      FROM user_tab_subpartitions s, user_segments u
      WHERE s.subpartition_name=u.partition_name
      AND u.segment_name='EVENT_LOG'
      AND s.table_name='EVENT_LOG') r
GROUP BY pname;
```

   - Multiply the output of this query by `31*0.8` (accounting for disk data compression by reducing memory by 20%).
   - This result provides the minimum required memory in bytes for one month.

Providing this calculated memory to In-Memory should prevent "Insufficient memory" messages when storing monthly `EVENT_LOG` data.

A.22 Upgrading 20.12 to 20.13 Fails on VMware With Error at Privileged Migrations Step

Learn how to resolve a privileged migrations error when upgrading from Oracle AVDF 20.12 to 20.13.

Problem

When upgrading from Oracle AVDF 20.12 to 20.13, the upgrade fails on VMware with the following error:

```
run-privileged-migrations ERROR - ODF-10001: Internal error: Fatal error
running migrations
```

Solution

To resolve this issue, first confirm that you are experiencing the same error. If so, follow the subsequent steps:

1. As the `root` user, check the integrity of the RPM database:

```
cd /var/lib/rpm
/usr/lib/rpm/rpmd_verify Packages
```

   If there are no errors, these instructions do not apply, contact Oracle Support.

2. If errors are found, execute the following commands to rebuild the RPM database:

```
cd /var/lib
cp -ax --backup=t rpm rpm.old
rm -i rpm/__db.???
rpm --rebuilddb
```

3. Once you have rebuilt the RPM database, check the validity of the rebuilt package database:

```
cd /var/lib/rpm
/usr/lib/rpm/rpmdb_verify Packages
```

4. Once confirmed, proceed with the upgrade according to the specific type of RPM database corruption encountered. Follow the appropriate steps based on the scenario experienced:
   - Resume the upgrade if the privileged migrations have not yet started:
     a. Reboot the system.
     b. Log in as the `root` user.
     c. Run the following command:

```
systemctl isolate avdf-upgrade.target
```

     d. To review the upgrade status, re-log in on the console as the `root` user.
   - Resume the upgrade after the privileged migrations have started:
     a. Apply the AVDF 20.13 update to the recovery utility:

```
rpm -U /media/avdf-install/bootstrap/Packages/avdf-
bootstrap-20.13.0.0.0-*.noarch.rpm
```

     b. Check the current status:

```
/opt/avdf/bin/privmigutl --status
```

     c. Review the output to find the failing migration and re-run it manually as the `root` user.
     d. Once the migration has completed successfully, run the following command:

```
/opt/avdf/bin/privmigutl --resume
```

A.23 Package Version Mismatch After Patching Leading to Perl Package Update Failure

Learn how to update various Perl packages which are causing issues when patching from Oracle AVDF 20.9 to newer versions.

Problem

After patching to AVDF 20.9, certain systems have an outdated set of Perl packages, such as `perl-interpreter`, `perl-libs`, and `perl-Utils`, which do not match versions available in a

fresh install. This mismatch does not introduce CVEs (as per Qualys reports) but could lead to dependency conflicts, especially when attempting further upgrades.

Solution

To resolve this package mismatch, uninstall the `Perl-devel` package and any other packages that depend on it, then manually upgrade the Perl packages using the following workaround:

1. Run the following command before beginning to patch:

   ```
   dnf remove perl-devel
   ```

2. Insert the upgrade ISO.
3. Mount it with `mount /dev/sr0 /images`.
4. Run the update command:

   ```
   /usr/bin/yum update --exclude=avs,dbfw-mgmtsvr -c /images/upgrade.repo
   ```

   This command erases the packages pre-patching, upgrades all the outdated Perl packages, aligning the system with the expected package set, and successfully resolves dependency conflicts.

B

Installing Oracle AVDF on Oracle Database Appliance (ODA)

Learn how to install Audit Vault Server or Database Firewall on Oracle Database Appliance.

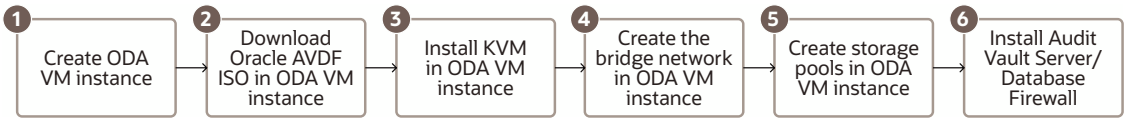
The Oracle Database Appliance (ODA) is a database server appliance. It is the easiest and most affordable way to run Oracle Databases and applications in remote and edge computing environments. It reduces Oracle Database deployment time and management workload using a pre-built integrated system with management automation.

Oracle AVDF comprises of Audit Vault Server and Database Firewall. They are delivered as software appliance images that can be deployed on physical machines or virtual machines (VM). Audit Vault Server and Database Firewall can be deployed on Oracle Database Appliance by creating a KVM (Kernel-based Virtual Machine) guest instance on ODA.

This appendix contains an overview for installing Audit Vault Server and Database Firewall on Oracle Database Appliance.

At the high level, below would be the flow of installation.

Figure B-1 Oracle AVDF on ODA



Follow these steps at a high level:

1. Prerequisites
   a. Create an ODA VM instance
   b. Download Oracle AVDF ISO files within the ODA VM instance
2. Install KVM on ODA VM instance
3. Install Audit Vault Server
   a. Create a storage pool for ISO files and Audit Vault Server installation
   b. Create a KVM guest instance
   c. Install Audit Vault Server or Database Firewall
4. Configure Audit Vault Server
   a. Deploy Audit Vault Agents
   b. Register the target database instance in the Audit Vault Server
   c. Start the Audit Vault Agent
   d. Configure the database instance as a target using the Audit Vault Server console
   e. Configure Auditing

f. Provision Audit Policies

g. Monitor Database Activity in Audit Vault Server

B.1 Completing the Installation Prerequisites

Learn about the prerequisites before the installation of Oracle AVDF on ODA.

1. Create an ODA VM instance by referring to *Oracle Database Appliance X8-2 Deployment and User's Guide*.

> **See Also:**
>
> Creating a Virtual Machine in a KVM Deployment

> **Note:**
>
> Oracle recommends to create a `vdisk` to accommodate the storage pools and attach the same to the VM.

This ODA VM instance is used as a hypervisor to host a nested VM for installing Oracle AVDF. The CPU mode in the ODA VM instance needs to be updated to support this nested virtualization.

2. Follow these steps to edit the CPU mode.

> **Note:**
>
> In these steps, `vm_name` is the ODA VM instance name and `vmstorage_name` is the `vmstorage` for this ODA VM instance.

a. Run the command:

```
virsh edit <vm_name>
```

b. Identify and spot the following lines in the XML file which need to be changed:

```
  <cpu mode='custom' match='exact' check='partial'>
```

c. Change the lines as follows:

```
<cpu mode='host-passthrough' check='none'/>
```

d. Save the XML file.

e. Copy the domain XML file (`/etc/libvirt/qemu/<vm_name>.xml`) to the ODA location `/u05/app/sharedrepo/<vmstorage_name>/.ACFS/snaps/vm_<vm_name>` by running the following command:

```
cp /etc/libvirt/qemu/<vm_name>.xml /u05/app/sharedrepo/
<vmstorage_name>/.ACFS/snaps/vm_<vm_name>
```

f. Restart the VM using these commands:

```
odacli stop-vm -n <vm_name>


odacli start-vm -n <vm_name>
```

3. Download the Oracle AVDF ISO files.

B.2 Download the Oracle AVDF ISO Files

Learn about downloading and verifying the software to install Oracle AVDF on ODA.

Download Oracle AVDF ISO files using the VNC console for the ODA VM instance. Refer to Downloading and Verifying Oracle AVDF Software for detailed steps for complete information.

Here are high level steps to follow:

1. 1 Open a web browser on the VNC console for ODA VM instance and go to the Oracle Software Delivery Cloud portal:

   https://edelivery.oracle.com

2. Click **Sign In**, and if prompted, enter your **User ID** and **Password**.
3. In the **All Categories** menu, select **Release**. In the following field, enter **Oracle Audit Vault and Database Firewall**, and then click **Search**.
4. Select the **Oracle Audit Vault and Database Firewall** version you want to install from the displayed list. Or click the **Select** icon that appears against the specific release.
5. In the next page, verify the details of the installation package, and then click **Continue**.
6. Read the **Oracle Standard Terms and Restrictions** displayed on the page. Select **I reviewed and accept the Oracle License Agreement** check box, and then click **Continue**.

> **Note:**
>
> Oracle AVDF release 20.3 and earlier, the Audit Vault Server installable files are available in parts and must be concatenated before installation. Starting with Oracle AVDF release 20.4, there is a single Audit Vault Server ISO file, and there is no need to concatenate.

The download page appears and displays the list of ISO files for *Oracle Audit Vault and Database Firewall*.

a. Audit Vault Server install: `Vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server

> **Note:**
>
> Starting Oracle AVDF 20.4, there is a single Audit Vault Server ISO file, and there is no need to concatenate.

b. Database Firewall install: `Vpart_number.zip` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Utilities.

7. Next to the **Print** button, click **View Digest Details**.

   The ISO files list expands to display each ISO file's SHA-1 and SHA-256 checksum reference numbers.

8. Verify the checksum value for all the ISO files.
9. Click **Download**. The **Download Manager Installation** screen is displayed. The size of the combined ISO files exceeds 11 GB, and takes time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.
10. Click **Download the installer**, and then click **Save File**.
11. Create a directory in ODA VM instance to download the ISO files. Download the ISO files into the ODA VM instance sources directory.
12. Click **Save**.
13. After the download is complete, launch a terminal session.
14. Check the ISO files have been downloaded correctly.

B.3 Installing KVM on ODA VM Instance for Running Oracle AVDF

Learn how to install KVM on ODA VM instance for running Oracle AVDF appliances.

Follow these steps to install KVM on the ODA VM instance, refer to the OS documentation about installing KVM hypervisor:

1. Run the following command to install the latest *qemu* packages and *virt-manager*:

   If ODA VM instance is OL7:

   ```
   yum -y install qemu-kvm qemu-img virt-manager libvirt libvirt-python
   libvirt-client virt-install
   ```

   If ODA VM instance is OL8:

   ```
   # yum install qemu-kvm qemu-img virt-manager libvirt libvirt-client virt-
   install
   ```

2. Run the following commands to enable *libvirtd*:

   ```
   systemctl enable libvirtd
   ```

   ```
   systemctl start libvirtd
   ```

3. Run the following commands to enable *tuned*:

```
systemctl enable tuned


systemctl start tuned


tuned-adm profile virtual-host
```

4. Enable nested VM support. Prior to ODA X10-2, ODA is Intel based and nested VM support is enabled by default. Starting from ODA X10-2 and above, ODA is AMD based, nested KVM support needs to be enabled manually by commenting out `options kvm_amd nested=0` on the ODA BM hosts. Make these changes in both BM hosts if using ODA high availabiliy model.

```
[root@ODABM root]# cat /etc/modprobe.d/kvm.conf
# Enable nested virtualization on Intel processorsoptions kvm_intel
nested=1
# Nested virtualization support on AMD processors is not stable enough
# for production use, so disable it
# options kvm_amd nested=0
```

5. Reboot BM host to make the changes effective.

B.4 Configuring the Network on ODA VM Instance

Learn how to configure a bridge network on ODA VM instance to be used by the Oracle AVDF VM instance.

The purpose of this section is to create a bridge network for ODA VM instance, attach the virtual interface to the bridge, and plumb IP to the bridge.

Refer to the Oracle Linux documentation for more details about how to configure the network.

Follow these steps:

1. From the bare metal host, access the ODA VM by using:

```
virsh <ODA VM name> --console
```

2. Create the bridge network:

```
< delete the existing ens3 configuration from network manager>
# nmcli connection down ens3
# nmcli connection delete ens3

<create a bridge br0 and add port ens3 to the bridge br0>
# nmcli connection add type bridge con-name br0 ifname br0
# nmcli connection add type ethernet slave-type bridge con-name br0-port1
ifname ens3 master br0

<configure IP, gateway, dns to the bridge>
# nmcli connection modify br0 ipv4.addresses 'x.x.x.x/xx'
# nmcli connection modify br0 ipv4.gateway 'y.y.y.y'
# nmcli connection modify br0 ipv4.dns 'x.x.x.x'
```

```
# nmcli connection modify br0 ipv4.dns-search 'example.com'
# nmcli connection modify br0 ipv4.method manual
```

B.5 Installing the Audit Vault Server on the ODA VM Instance

Learn how to install the Audit Vault Server or Database Firewall on the ODA VM instance.

The ODA VM instance was installed following the steps in the previous topic.

Follow these steps on a high level to install Audit Vault Server or Database Firewall on the ODA VM instance

1. Create a storage pool to upload ISO files.
2. Create a storage pool for installing Audit Vault Server
3. Create a KVM guest instance
4. Install the Audit Vault Server

Follow these steps to create a storage pool in the ODA VM instance to upload Oracle AVDF ISO files:

1. Connect to the Virtual Machine using the VNC Viewer as *root* user.
2. Open a terminal and launch the *virt-manager*.
3. Right click on **QEMU/KVM**. Choose **Details**, and then select the **Storage** tab.
4. In the **Storage** tab of the *virt-manager*, click the plus button in the bottom left corner.
5. Provide a **Name** from which you can quickly identify that it is for the installable ISO file.
6. Select the **Type** of the storage pool. For example: `dir: Filesystem Directory`.
7. Provide the **Target Path**. It is the directory where the Audit Vault Server ISO files will be stored. For example: `/u01/source/av`.
8. Click **Finish**.
9. The newly created storage pool appears on the left hand side. Select the pool.
10. Copy or move the ISO file to this storage pool.

Follow these steps to create a storage pool for installing Audit Vault Server or Database Firewall. The appliance is installed on the storage pool.

1. Connect to the Virtual Machine with VNC Viewer as the *root* user.
2. Open a terminal and launch *virt-manager*.
3. Right-click on **QEMU/KVM**. Then choose **Details** and select the **Storage** tab.
4. Click the plus button in the bottom left corner.
5. Provide a **Name**.
6. Select the **Type** of the storage pool. For example: `dir: Filesystem Directory`.
7. Provide the **Target Path**. It is the directory where Audit Vault Server files are stored. For example: `/u01/kvm/av`.
8. Click **Finish**.
9. The new directory created appears on the left-hand side. Select the directory and then click the plus button next to **Volumes**.
10. Enter the **Name**.

11. Select the **Format** as `qcow2`.
12. Specify the size in the **Max Capacity** field. This is for installing Audit Vault Server, which requires a minimum of 256 GB.
13. Click **Finish**.
14. The newly created entry appears in the table below the **Volumes** field. Verify the same.

Follow these steps to create a KVM guest instance. KVM can be managed through the command line or GUI tools. In this document, the focus is on using the GUI tools. Use VNC console to connect to the ODA VM instance. Open the **gnome-terminal** and follow the steps or commands.

1. Connect to the Virtual Machine with VNC Viewer as the *root* user.
2. Open a terminal and launch *virt-manager*.
3. Select **File** and select **New Virtual Machine**.
4. Select the `Local install media (ISO image or CDROM)` option.
5. In the next few steps, choose the options based on the configuration, which may differ. Select the `Use ISO image` option and click **Browse** to select the first ISO file.
6. Deselect the checkbox **Automatically detect operating system based on install media**.
7. Select `Linux` as the **OS Type**.
8. Choose the **Version**. For example, `Oracle Linux 7.7`.
9. Choose **Memory** and **CPU settings** based on the workload of the service used on this KVM guest virtual machine. For example, `16384` MB as **Memory (RAM)** and **CPUs** as `4`.
10. Click **Forward**.
11. Select the radio button **Select or create custom storage**.
12. Enter the path of the storage pool created earlier. For example: `/u01/kvm/av/av191.qcow2`.
13. In the **New VM** dialog, enter the **Name**.
14. Select the **Customize configuration before install** field.
15. Expand the **Network selection** area, and select the previously created bridge.
16. Select `virtio` in the **Device model** field.
17. Add the **MAC address** of the vNIC, and click **Apply**.
18. Click **VirtIO Disk1** on the left, and expand **Advanced Options**.
19. Select `SATA` in the **Disk bus** field.
20. Click **IDE CDROM 1** on the left, and ensure the **Source path** has the correct ISO file.
21. Select `SATA` in the **Disk bus** field.21. Click **VirtIO Disk1** on the left, and expand **Advanced Options**.
22. Click **Begin Installation** in the top left corner of the dialog.

The virtual machine starts the installation and detects the vNIC network device attached to the virtual machine. The installation takes approximately one hour to complete. See Installing Audit Vault Server or Database Firewall for more information.

1. The system boots, and the initial splash screen appears. This indicates the Oracle AVDF release is being installed.

2. Enter the new *root* user password when prompted for change. Enter the same password when prompted for confirmation.
3. See Post-Install Configuration Tasks for more information on the installation passphrase used for initial log in to the Audit Vault Server console.
4. When prompted to insert the installation ISO again to continue, go to the KVM console.
5. Click **View** and then **Details**.
6. Click **IDE CDROM1** on the left. In the **Source path** field, click **Connect** to specify the ISO file path.
7. Select the `Image Location` option and click **Browse** to navigate and select the ISO file.
8. Click **Choose Volume**.
9. Click the terminal icon to switch to the installation console.
10. Log in as *root* user to continue with the installation.
11. Select the default network interface. Ensure the MAC address is correct.
12. Set up the network configuration by entering the following fields:
    - **IP address**: Enter the IP address that is used for Audit Vault Server installation.
    - **Network mask**
    - **Gateway**: Enter the IP address of the network interface if a gateway is required. Else, clear the field before saving.
13. Press the **Tab** key to navigate to the **OK** button, and press the **Enter** button. The installation begins and may take up to two hours to complete.
14. A confirmation message is displayed on the screen after the installation is completed. Click **OK**.
15. In the host VM instance, open a web browser. Enter `https://<VM Private IP address of the vNIC assigned to Oracle AVDF VM>/console`.
16. Choose to accept and continue to connect to the Audit Vault Server console.
17. Enter the password chosen earlier to log in.
18. When prompted, enter the user name of the *super administrator* and *super auditor*. Set the repository encryption password, *support* user password (for SSH access to VM), *root* user password (for *root* privilege on the VM). See Accessing the Audit Vault Server Post-Install Configuration Page for more information.
19. Expand the **Time Setup** region, and select `Use NTP`. Enter **Server 1** IP address and click **Test Server**.

    Note: Time difference between the Audit Vault Server and target negatively impacts the audit collection.
20. Check the network connectivity between the Audit Vault Server and targets by using ICMP ping. If all the previous steps were correctly performed, the Audit Vault Server and targets will connect with each other.

B.6 Installing the Database Firewall on the ODA VM Instance

Learn how to install the Database Firewall on ODA (Oracle Database Appliance) VM instance.

Follow the same steps documented in the previous section Installing the Audit Vault Server on the ODA VM Instance pointing to the Database Firewall ISO.

After the Database Firewall VM is ready, you need to follow additional steps to register the Database Firewall.

Additionally, follow these steps:

1. Register the Database Firewall in the Audit Vault Server console. See Specifying the Audit Vault Server Certificate and IP Address for more information.
2. Log in to the Audit Vault Server console as an *administrator*.
3. Click the **Settings** tab.
4. Click the **Security** tab in the left navigation menu.
5. Click the **Certificate** tab on the main page, and then click the **Server Certificate** sub tab. The server's certificate is displayed.
6. Copy the server's certificate.
7. Connect to the Database Firewall server through SSH as a *support* user.
8. Switch to *root* user:

   ```
   su - root
   ```

9. Copy the certificate of the Audit Vault Server into a file: `vi /root/certif_avs.crt`.
10. Run the following command to associate the primary Audit Vault Server to the Database Firewall:

    ```
    cat /root/certif_avs.crt | /opt/avdf/config-utils/bin/config-avs set
    avs=primary address=<IP address of the primary AVS> certificate=<Path of
    the certificate>
    ```

11. Run the following command to synchronize the system clocks of Database Firewall Server with the Audit Vault Server:

    ```
    /opt/avdf/config-utils/bin/config-ntp set servers=<Comma separated IP
    addresses or hostnames of NTP servers> sync_on_save=true enabled=true
    ```

12. In the Audit Vault Server console, navigate to the **Database Firewalls** tab.
13. Click **Register**.
14. Enter a **Name** and **IP Address** in the dialog.
15. Click **Save**. The Database Firewall instance is registered and is displayed in the list.