CIS VMware vSphere 7.0 vCenter Appliance PostgreSQL STIG Benchmark

v1.0.0 - 08-20-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

VMware vSphere 7.0 vCenter Appliance PostgreSQL Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 26 Jul 2023

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware vSphere 7.0 vCenter Appliance PostgreSQL and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for VMware vSphere 7.0 vCenter Appliance PostgreSQL

Recommendations

1 STIG RULES

VMware vSphere 7.0

VMware vSphere 7.0 vCenter Appliance PostgreSQL Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 26 Jul 2023

CLASSIFICATION unclassified

1.1 VCPG-70-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must limit the number of connections.

```
GROUP ID: V-256591
RULE ID: SV-256591r887559
```

Rationale:

Database management includes the ability to control the number of users and user sessions utilizing a database management system (DBMS). Unlimited concurrent connections to the DBMS could allow a successful denial-of-service (DoS) attack by exhausting connection resources, and a system can also fail or be degraded by an overload of legitimate users. Limiting the number of concurrent sessions per user is helpful in reducing these risks.

VMware Postgres as deployed on the vCenter Service Appliance (VCSA) comes preconfigured with a "max_connections" limit that is appropriate for all tested, supported scenarios. The out-of-the-box configuration is dynamic, based on a lower limit plus allowances for the resources assigned to VCSA and the deployment size. However, this number will always be between 100 and 1000 (inclusive).

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
max_connections;"
```

If the returned number is not greater than or equal to 100 and less than or equal to 1000, this is a finding.

Remediation:

At the command prompt, run the following command:

```
# vmon-cli --restart vmware-vpostgres
```

Note: Restarting the service runs the "pg_tuning" script that will configure "max_connections" to the appropriate value based on the allocated memory for vCenter.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.2 VCPG-70-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres log files must contain required fields.

```
GROUP ID: V-256592
RULE ID: SV-256592r887562
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

As an embedded database that is only accessible via "localhost", VMware Postgres on the vCenter Server Appliance (VCSA) does not implement robust auditing. However, it can and must be configured to log reasonable levels of information relating to user actions to enable proper troubleshooting.

Satisfies: SRG-APP-000089-DB-000064, SRG-APP-000095-DB-000039, SRG-APP-000096-DB-000040, SRG-APP-000097-DB-000041, SRG-APP-000098-DB-000042, SRG-APP-000099-DB-000043, SRG-APP-000100-DB-000201, SRG-APP-000101-DB-000044, SRG-APP-000375-DB-000323

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
log_line_prefix;"
```

Expected result:

```
%m %c %x %d %u %r %p %l
```

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
log_line_prefix TO '%m %c %x %d %u %r %p %l ';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 f

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

1.3 VCPG-70-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres configuration files must not be accessible by unauthorized users.

```
GROUP ID: V-256593
RULE ID: SV-256593r887565
```

Rationale:

VMware Postgres has a few configuration files that directly control the security posture of the database management system (DBMS). Protecting these files from unauthorized access and modification is fundamental to ensuring the security of VMware Postgres.

Satisfies: SRG-APP-000090-DB-000065, SRG-APP-000121-DB-000202, SRG-APP-000122-DB-000203, SRG-APP-000123-DB-000204, SRG-APP-000380-DB-000360

Audit:

At the command prompt, run the following command:

```
# find /storage/db/vpostgres/*conf* -xdev -type f -a '(' -not -perm 600 -o -
not -user vpostgres -o -not -group vpgmongrp ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# chmod 600 <file>
# chown vpostgres:vpgmongrp <file>
```

Note: Replace with the file that has incorrect permissions.

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

1.4 VCPG-70-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must be configured to overwrite older logs when necessary.

```
GROUP ID: V-256594
RULE ID: SV-256594r887568
```

Rationale:

Without proper configuration, log files for VMware Postgres can grow without bound, filling the partition and potentially affecting the availability of the vCenter Server Appliance (VCSA). One part of this configuration is to ensure the logging subsystem overwrites, rather than appends to, any previous logs that would share the same name. This is avoided in other configuration steps, but this best practice should be followed for good measure.

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
log_truncate_on_rotation;"
```

Expected result:

on

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
log_truncate_on_rotation TO 'on';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

1.5 VCPG-70-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The VMware Postgres database must protect log files from unauthorized access and modification.

```
GROUP ID: V-256595
RULE ID: SV-256595r887571
```

Rationale:

If audit data were to become compromised, competent forensic analysis and discovery of the true source of potentially malicious system activity would be difficult, if not impossible, to achieve. In addition, access to audit records provides information an attacker could use to their advantage.

To ensure the veracity of audit data, the information system and/or the application must protect audit information from all unauthorized access. This includes read, write, copy, etc.

Satisfies: SRG-APP-000118-DB-000059, SRG-APP-000119-DB-000060, SRG-APP-000120-DB-000061

Audit:

At the command prompt, run the following command:

```
# find /var/log/vmware/vpostgres/* -xdev -type f -a '(' -not -perm 600 -o -
not -user vpostgres -o -not -group vpgmongrp ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# chmod 600 <file>
# chown vpostgres:vpgmongrp <file>
```

Note: Replace `<file>` with the file that has incorrect permissions.

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
log_file_mode TO '0600';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.6 VCPG-70-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All vCenter database (VCDB) tables must be owned by the "vc" user account.

```
GROUP ID: V-256596
RULE ID: SV-256596r918971
```

Rationale:

Within the database, object ownership implies full privileges to the owned object, including the privilege to assign access to the owned objects to other subjects. Database functions and procedures can be coded using definer's rights. This allows anyone who uses the object to perform the actions if they are the owner. If not properly managed, this can lead to privileged actions being taken by unauthorized individuals.

VCDB is configured out of the box to be owned by the "vc" Postgres user. This configuration must be verified and maintained.

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres -t -A -c "\dt;"
| grep -v 'table|vc'
```

If any tables are returned, this is a finding.

Note: Upgrades may introduce new tables that are owned by the "postgres" user and can be updated to be owned by the "vc" user.

Remediation:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres -c "ALTER TABLE
<tablename> OWNER TO vc;"
```

Replace `<tablename>` with the name of the table discovered during the check.

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.7 VCPG-70-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must limit modify privileges to authorized accounts.

```
GROUP ID: V-256597
RULE ID: SV-256597r887577
```

Rationale:

If VMware Postgres were to allow any user to make changes to database structure or logic, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

Only qualified and authorized individuals must be allowed to obtain access to information system components to initiate changes, including upgrades and modifications.

Unmanaged changes that occur to the database software libraries or configuration can lead to unauthorized or compromised installations.

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "\du;"|grep "Create"
```

Expected result:

```
 postgres   | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 vc         | Create DB                                                  | {}
 vlcmuser   | Create DB                                                  | {}
```

If accounts other than "postgres","vc", and "vlcmuser" have any "Create" privileges, this is a finding.

Remediation:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "REVOKE ALL
PRIVILEGES FROM <user>;"
```

Replace `<user>` with the account discovered during the check.

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.8 VCPG-70-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must be configured to use the correct port.

```
GROUP ID: V-256598
RULE ID: SV-256598r887580
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports, protocols, and services on information systems.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the application must support the organizational requirements providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Database Management Systems using ports, protocols, and services deemed unsafe are open to attack through those ports, protocols, and services. This can allow unauthorized access to the database and through the database to other components of the information system.

Satisfies: SRG-APP-000142-DB-000094, SRG-APP-000383-DB-000364

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW port;"
```

Expected result:

5432

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
port TO '5432';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.9 VCPG-70-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

VMware Postgres must require authentication on all connections.

```
GROUP ID: V-256599
RULE ID: SV-256599r887583
```

Rationale:

To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

VMware Postgres client authentication configuration is configured in "pg_hba.conf". In this file are a number of lines that specify who can connect to the service, from where, and using what authentication methods. In Postgres there is a concept of a trusted connection where a specific network mask can connect without any authentication to any account. This connection is termed "trust" in "pg_hba.conf", and it must not be present. Out of the box, VMware Postgres requires standard password authentication for all connections.

Audit:

At the command prompt, run the following command:

```
# grep -v "^#" /storage/db/vpostgres/pg_hba.conf|grep -z --color=always
"trust"
```

If any lines are returned, this is a finding.

Remediation:

Navigate to and open /storage/db/pgdata/pg_hba.conf.

Find and remove the line that has a method of "trust" in the far-right column.

A correct, typical line will look like the following:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD
host       all          all                 127.0.0.1/32           md5
```

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

1.10 VCPG-70-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vPostgres database must use "md5" for authentication.

```
GROUP ID: V-256600
RULE ID: SV-256600r887586
```

Rationale:

The DOD standard for authentication is DOD-approved public key infrastructure (PKI) certificates.

Authentication based on user ID and password may be used only when it is not possible to employ a PKI certificate, and requires authorizing official approval.

In such cases, database passwords stored in clear text, using reversible encryption or unsalted hashes, would be vulnerable to unauthorized disclosure. Database passwords must always be in the form of one-way, salted hashes when stored internally or externally to the database management system (DBMS).

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
password_encryption;"
```

Expected result:

md5

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
password_encryption TO 'md5';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)

1.11 VCPG-70-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

VMware Postgres must be configured to use Transport Layer Security (TLS).

```
GROUP ID: V-256601
RULE ID: SV-256601r887589
```

Rationale:

The DOD standard for authentication is DOD-approved public key infrastructure (PKI) certificates. Authentication based on user ID and password may be used only when it is not possible to employ a PKI certificate.

In such cases, passwords, must be protected at all times, and encryption is the standard method for protecting passwords during transmission.

VMware Postgres is configured out of the box to require TLS connections with remote clients. As an embedded database and available only on "localhost" for standalone vCenter Server Appliances (VCSAs), TLS connections are used only in high-availability deployments for connections between a primary and a standby. This configuration must be verified and maintained.

Satisfies: SRG-APP-000172-DB-000075, SRG-APP-000442-DB-000379

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW ssl;"
```

Expected result:

on

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET ssl
TO 'on';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)
- NIST SP 800-53 Revision 5::IA-5 (1) (c)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

1.12 VCPG-70-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

VMware Postgres must enforce authorized access to all public key infrastructure (PKI) private keys.

```
GROUP ID: V-256602
RULE ID: SV-256602r887592
```

Rationale:

The DOD standard for authentication is DOD-approved PKI certificates. PKI certificate-based authentication is performed by requiring the certificate holder to cryptographically prove possession of the corresponding private key.

If a private key is stolen, an attacker can use it to impersonate the certificate holder. In cases where the database management system (DBMS)-stored private keys are used to authenticate the DBMS to the system's clients, loss of the corresponding private keys would allow an attacker to successfully perform undetected man-in-the-middle attacks against the DBMS system and its clients.

All access to the private key(s) of the DBMS must be restricted to authorized and authenticated users.

Audit:

At the command prompt, run the following command:

```
# stat -c "%a:%U:%G" /storage/db/vpostgres_ssl/server.key
```

Expected result:

600:vpostgres:vpgmongrp

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# chmod 600 /storage/db/vpostgres_ssl/server.key
# chown vpostgres:vpgmongrp /storage/db/vpostgres_ssl/server.key
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.13 VCPG-70-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

VMware Postgres must use FIPS 140-2 approved Transport Layer Security (TLS) ciphers.

```
GROUP ID: V-256603
RULE ID: SV-256603r887595
```

Rationale:

Use of weak or unvalidated cryptographic algorithms undermines the purposes of using encryption and digital signatures to protect data. Weak algorithms can be broken, and unvalidated cryptographic modules may not implement algorithms correctly. Unapproved cryptographic modules or algorithms should not be relied on for authentication, confidentiality, or integrity. Weak cryptography could allow an attacker to gain access to and modify data stored in the database as well as the administration settings of the database management system (DBMS).

VMware Postgres does not currently implement FIPS-validated cryptographic modules. This is planned but, in the interim, Postgres can be configured with strong ciphers from the FIPS-140 approved suite. Additionally, as an embedded database available only on "localhost" for a standalone vCenter Server Appliance, TLS connections are used only in high-availability deployments for connections between a primary and a standby.

Satisfies: SRG-APP-000179-DB-000114, SRG-APP-000514-DB-000381, SRG-APP-000514-DB-000382, SRG-APP-000514-DB-000383

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
ssl_ciphers;"
```

Expected result:

```
!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH
```

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
ssl_ciphers TO '!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.14 VCPG-70-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must write log entries to disk prior to returning operation success or failure.

```
GROUP ID: V-256604
RULE ID: SV-256604r887598
```

Rationale:

Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Preserving system state information helps to facilitate system restart and return to the operational mode of the organization with less disruption of mission/business processes.

Aggregating log writes saves on performance but leaves a window for log data loss. The logging system inside VMware Postgres is capable of writing logs to disk fully and completely before the associated operation is returned to the client. This ensures database activity is always captured, even in the event of a system crash during or immediately after a given operation.

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SELECT
name,setting FROM pg_settings WHERE name IN
('fsync','full_page_writes','synchronous_commit');"
```

Expected result:

```
fsync              | on
full_page_writes   | on
synchronous_commit | on
```

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands for each setting returned as "off" in the check:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
<name> TO 'on';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Note: Substitute with the incorrectly set parameter (fsync, full_page_writes, synchronous_commit).

Additional Information:

CCI-001665 Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (v)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-24

1.15 VCPG-70-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must not allow schema access to unauthorized accounts.

```
GROUP ID: V-256605
RULE ID: SV-256605r887601
```

Rationale:

Database management systems typically separate security functionality from nonsecurity functionality via separate databases or schemas. Database objects or code implementing security functionality should not be commingled with objects or code implementing application logic. When security and nonsecurity functionality are commingled, users who have access to nonsecurity functionality may be able to access security functionality.

VMware Postgres contains a number of system configuration schemas for which access must be strictly limited. By default, the "pg_catalog" and "information_schema" objects are configured to only be accessible in a read-only manner publicly and otherwise only accessible by the Postgres user. This configuration must be verified and maintained.

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "\dp .*.;" |grep -E
"information_schema|pg_catalog"|awk -F '|' '{print $4}'|awk -F '/' '{print
$1}'|grep -v "=r" | grep -v "^[[:space:]]*$" | grep -v "postgres"
```

If any lines are returned, this is a finding.

Remediation:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "REVOKE ALL
PRIVILEGES ON <name> FROM <user>;"
```

Replace <name> and <user> with the Access Privilege name and account, respectively, discovered during the check.

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

1.16 VCPG-70-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must provide nonprivileged users with minimal error information.

```
GROUP ID: V-256606
RULE ID: SV-256606r887604
```

Rationale:

Any database management system (DBMS) or associated application providing too much information in error messages on the screen or printout risks compromising the data and security of the system. The structure and content of error messages must contain the minimal amount of information.

Databases can inadvertently provide a wealth of information to an attacker through improperly handled error messages. In addition to sensitive business or personal information, database errors can provide host names, IP addresses, user names, and other system information not required for troubleshooting but very useful to someone targeting the system.

Satisfies: SRG-APP-000266-DB-000162, SRG-APP-000267-DB-000163

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
client_min_messages;"
```

Expected result:

notice

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
client_min_messages TO 'notice';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

1.17 VCPG-70-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must have log collection enabled.

```
GROUP ID: V-256607
RULE ID: SV-256607r887607
```

Rationale:

Without the ability to centrally manage the content captured in the audit records, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

The content captured in audit records must be managed from a central location (necessitating automation). Centralized management of audit records and logs provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records.

VMware Postgres is capable of outputting directly to syslog but for performance reasons, the vCenter Server Appliance (VCSA) is configured to ship logs centrally via "rsyslog" file monitoring. To facilitate that configuration, log files must be generated to disk.

Satisfies: SRG-APP-000356-DB-000314, SRG-APP-000356-DB-000315, SRG-APP-000092-DB-000208, SRG-APP-000381-DB-000361, SRG-APP-000495-DB-000326, SRG-APP-000495-DB-000327, SRG-APP-000495-DB-000328, SRG-APP-000495-DB-000329, SRG-APP-000496-DB-000334, SRG-APP-000496-DB-000335, SRG-APP-000499-DB-000330, SRG-APP-000499-DB-000331, SRG-APP-000501-DB-000336, SRG-APP-000501-DB-000337, SRG-APP-000504-DB-000354, SRG-APP-000504-DB-000355, SRG-APP-000507-DB-000356, SRG-APP-000507-DB-000357, SRG-APP-000508-DB-000358

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
logging_collector;"
```

Expected result:

on

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
logging_collector TO 'on';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

CCI-001844 The information system provides centralized management and configuration of the content to be captured in audit records generated by organization-defined information system components.

- NIST SP 800-53 Revision 4::AU-3 (2)

1.18 VCPG-70-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must be configured to log to "stderr".

```
GROUP ID: V-256608
RULE ID: SV-256608r887610
```

Rationale:

Without the ability to centrally manage the content captured in the audit records, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

The content captured in audit records must be managed from a central location (necessitating automation). Centralized management of audit records and logs provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records.

For VMware Postgres logs to be successfully sent to a remote log management system, log events must be sent to "stderr". Those events will be captured and logged to disk where they will be picked up by "rsyslog" for shipping.

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
log_destination;"
```

Expected result:

stderr

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
log_destination TO 'stderr';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

1.19 VCPG-70-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

"Rsyslog" must be configured to monitor VMware Postgres logs.

```
GROUP ID: V-256609
RULE ID: SV-256609r887613
```

Rationale:

For performance reasons, "rsyslog" file monitoring is preferred over configuring VMware Postgres to send events to a "syslog" facility. Without ensuring that logs are created, that "rsyslog" configs are created, and that those configs are loaded, the log file monitoring and shipping will not be effective.

Satisfies: SRG-APP-000359-DB-000319, SRG-APP-000360-DB-000320, SRG-APP-000515-DB-000318

Audit:

At the command prompt, run the following command:

```
# rpm -V VMware-Postgres-cis-visl-scripts|grep -E "vmware-services-vmware-
vpostgres.conf|vmware-services-vmware-postgres-archiver.conf" | grep
"^..5......"
```

If the command returns any output, this is a finding.

Remediation:

Navigate to and open:

/etc/vmware-syslog/vmware-services-vmware-vpostgres.conf

Create the file if it does not exist.

Set the contents of the file as follows:

```
# vmware-vpostgres first logs, before loading configuration
input(type="imfile"
      File="/var/log/vmware/vpostgres/serverlog.std*"
      Tag="vpostgres-first"
      Severity="info"
      Facility="local0")
# vmware-vpostgres logs
input(type="imfile"
      File="/var/log/vmware/vpostgres/postgresql-*.log"
      Tag="vpostgres"
      Severity="info"
      Facility="local0")
```

Navigate to and open:

/etc/vmware-syslog/vmware-services-vmware-postgres-archiver.conf

Create the file if it does not exist.

Set the contents of the file as follows:

```
# vmware-postgres-archiver logs
input(type="imfile"
      File="/var/log/vmware/vpostgres/pg_archiver.log.std*"
      Tag="postgres-archiver"
      Severity="info"
      Facility="local0")
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

1.20 VCPG-70-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VMware Postgres must use Coordinated Universal Time (UTC) for log timestamps.

```
GROUP ID: V-256610
RULE ID: SV-256610r887616
```

Rationale:

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis. Time stamps generated by VMware Postgres must include date and time expressed in UTC, a modern continuation of Greenwich Mean Time (GMT).

Audit:

At the command prompt, run the following command:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
log_timezone;"
```

Expected result:

Etc/UTC

If the output does not match the expected result, this is a finding.

Remediation:

At the command prompt, run the following commands:

```
# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "ALTER SYSTEM SET
log_timezone TO 'Etc/UTC';"

# /opt/vmware/vpostgres/current/bin/psql -U postgres -c "SELECT
pg_reload_conf();"
```

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCPG-70-000001 (Manual)	☐	☐
1.2	VCPG-70-000002 (Manual)	☐	☐
1.3	VCPG-70-000003 (Manual)	☐	☐
1.4	VCPG-70-000004 (Manual)	☐	☐
1.5	VCPG-70-000005 (Manual)	☐	☐
1.6	VCPG-70-000006 (Manual)	☐	☐
1.7	VCPG-70-000007 (Manual)	☐	☐
1.8	VCPG-70-000008 (Manual)	☐	☐
1.9	VCPG-70-000009 (Manual)	☐	☐
1.10	VCPG-70-000010 (Manual)	☐	☐
1.11	VCPG-70-000011 (Manual)	☐	☐
1.12	VCPG-70-000012 (Manual)	☐	☐
1.13	VCPG-70-000013 (Manual)	☐	☐
1.14	VCPG-70-000014 (Manual)	☐	☐
1.15	VCPG-70-000015 (Manual)	☐	☐
1.16	VCPG-70-000016 (Manual)	☐	☐
1.17	VCPG-70-000017 (Manual)	☐	☐
1.18	VCPG-70-000018 (Manual)	☐	☐
1.19	VCPG-70-000019 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	VCPG-70-000020 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 20, 2025	1.0.0	Initial CIS Release