Micro Focus International, PLC

Vertica Analytic Database

Database SRG Compliance Guide v2r10

Document Version: 0.6

Prepared for:

Micro Focus International, PLC
150 Cambridgepark Dr
Cambridge, MA 02140
United States of America

Phone: +1 617 386 4400
www.microfocus.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This document details the Micro Focus International, PLC (Micro Focus) Vertica Analytic Database compliance with Database SRG[1] v2r10. Vertica Analytic Database is a high-performance, massively parallel processing SQL[2] engine with advanced analytics and machine learning.

1.1 Purpose

DISA[3] Risk Management Executive (RME) developed the Database SRG to ensure secure deployment and configuration of products within the Department of Defense Information Network (DoDIN). SRGs contain generalized requirements for particular product types. Mapping the generalized requirements to a specific product to achieve compliance proves to be a challenge. This guide provides configurations and mitigations for the Vertica Analytic Database to meet all Database SRG v2r10 requirements. Use this document as a guiding document for installation and administration of Vertica when deployed within the DoDIN. Only refer to Micro Focus Vertica documentation as directed within this document.

Vertica documentation can be found online at https://www.vertica.com/documentation/vertica/9-2-x-documentation/ .

1.2 Target Audience

The audience for this document consists of the end-user, the Micro Focus development staff, and Information System Security Managers (ISSMs) within the Department of Defense.

1.3 Document Conventions

The following font conventions are used throughout this document:

- **Vertica** documentation sections are in **bold** font
- *Files* on the system are in *italics*
- `System directories` are in `Courier New` font
- <*database specific*> portions of commands are in *italics* within < >
- Database ROLES are in all caps
- Database users are in all lower case

1.4 Vertica Deployment Scenarios

Vertica supports a number of deployment scenarios. This document describes configuration details specific to these deployment scenarios:

- Single instance embedded
- Single instance stand-alone

[1] SRG – Security Requirements Guide
[2] SQL – Structured Query Language
[3] DISA – Defense Information Systems Agency

- Multi-node cluster

1.5 Assumptions

The writers of this document assume the following:

- Deployment scenario:
  - Physically secured in locked computer room, or switch cabinet;
  - Located behind the enclave firewall;
  - Administrative access restricted to management VLAN[4].

1.6 Required Ports

When deployed in a cluster, Vertica communicates between nodes using Spread for control messaging on the state of the nodes. Data is shared between nodes using a TCP[5] data channel. Vertica communicates with external components over TLS[6] and SSH[7]. Please ensure your network's firewall settings allow communications using the following ports:

Table 1 – Vertica Required Ports

Port	Inbound/ Outbound	Protocol	Service	Description
22	Inbound	TCP	SSH	Secure administration of Vertica over SSH when Administration Tools are enabled.
53	Inbound/ Outbound	UDP[8]	DNS	DNS resolver
5433	Outbound	TCP	Kafka	Notifiers send Data Collector tables to Kafka server.
4803	Inbound/ Outbound	TCP	Spread	Spread client connections for inter-cluster communications.
4803	Inbound/ Outbound	UDP	Spread	Spread daemon to daemon communications within the cluster.
4804	Inbound/ Outbound	UDP	Spread	Spread daemon to daemon communications within the cluster.
5433	Inbound	TCP	Vertica	Vertica client communications (vsql, ODBC, JDBC).
5433	Inbound/ Outbound	UDP	Vertica	Vertica spread monitoring when used as a cluster.

[4] VLAN – Virtual Local Area Network
[5] TCP – Transmission Control Protocol
[6] TLS – Transport Layer Security
[7] SSH – Secure Shell
[8] UDP – User Datagram Protocol

Port	Inbound/ Outbound	Protocol	Service	Description
5434	Inbound/ Outbound	TCP	Vertica	Intra- and inter-cluster communications, such as during a plan.
6543	Inbound/ Outbound	UDP	Spread	Monitoring the Spread daemon connections.
14159 – 14161	Inbound	TCP	vnetperf	vnetperf utility measures network performance of cluster hosts
50000	Inbound/ Outbound	TCP	rsync	rync daemon that is used in database backup
All	Inbound/ Outbound	ICMP[9]	ICMP	ICMP requests and echoes within the cluster subnet

All ports not listed in Table 1 shall be closed to meet SRG-APP-000383-DB-000364 or documented in the Ports, Protocols, and Services Management (PPSM) Registry.

[9] ICMP – Internet Control Message Protocol

2. Installation Procedure

Micro Focus provides guidance for how to properly install Vertica in the **Installing Vertica** section of the Vertica documentation. For additional guidance on these steps, refer to the Section **Installing Manually** (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/InstallationGuide/Other/InstallingManually.htm).

For most configurations, Vertica will be deployed as a cluster on dedicated hosts. No other software should be installed on the Vertica hosts. In some instances, Vertica is embedded within an OEM[10] appliance. In these instances, only the OEM's application shall be allowed access to the Vertica database. No direct access by users is permitted.

The administrator should ensure the following items are acquired before installation:

- Required Ancillary Equipment. The following can be used to meet some of the database requirements:
  - LDAP over TLS can be used to meet the following requirements:
    - SRG-APP-000175-DB-000067
    - SRG-APP-000177-DB-000069
    - SRG-APP-000427-DB-000385
  - Self-encrypting drives (if needed)
    - SRG-APP-000231-DB-000154
    - SRG-APP-000428-DB-000386
    - SRG-APP-000429-DB-000387
  - Centralized audit server
    - SRG-APP-000356-DB-000314
    - SRG-APP-000359-DB-000319
    - SRG-APP-000360-DB-000320
  - Apache Kafka server to facilitate sending Data Collector tables to a centralized audit server.
    - SRG-APP-000515-DB-000318
- Network Configuration details:
  - Apache Kafka server IP[11] address
  - Syslog Server address
  - LDAP
    - IP address
    - Certificate
    - Path to Certificate Authority (CA) certificate
    - Bind account details

By default, Vertica installs in the `/opt/vertica/*` directory. No other software is allowed in this directory. This separation meets SRG-APP-000133-DB-000199.

[10] OEM – Original Equipment Manufacturer
[11] IP – Internet Protocol

2.1 Additions to Initial Configuration

The **Vertica Installation Guide** details how to perform initial configuration of the system. This section describes how to adjust some of the options to ensure the tested configuration meets DISA requirements.

Demonstration or sample databases must be removed (SRG-APP-000141-DB-000090 and SRG-APP-000141-DB-000091 and SRG-APP-000243-DB-000128):

- Run the following commands and check the output to ensure no test or example data is present:

  SELECT * from schemata where is_system_schema = 'f';

  Review results for example or test schemas and remove any found.
- In `/opt/vertica/share` only the following samples should be present
  - vertica.conf.sample
  - debug_log.conf.sample

  These files are necessary to create new databases and are not samples.
- The following can be used to remove the remaining unnecessary components once installation is complete:

```
/opt/vertica/packages/approximate
/opt/vertica/packages/AWS
/opt/vertica/packages/hcat
/opt/vertica/packages/logsearch
/opt/vertica/packages/MachineLearning
/opt/vertica/packages/ParquetExport
/opt/vertica/packages/place
/opt/vertica/packages/SparkConnector
/opt/vertica/packages/VFunctions
/opt/vertica/packages/voltagesecure
/opt/vertica/packages/flextable/examples
/opt/vertica/packages/kafka/examples
/opt/vertica/packages/kafka/examples/example_event.json
/opt/vertica/packages/txtindex/examples
/opt/vertica/sbin/agent_restart
/opt/vertica/sbin/agent_stop
/opt/vertica/sbin/install_example
/opt/vertica/sbin/delete_example
/opt/vertica/sbin/build_vertica_keyless_ssh
/opt/vertica/sbin/check_firewall_status
/opt/vertica/sbin/cluster_clean_node
/opt/vertica/sbin/configure_admintools
/opt/vertica/sbin/configure_aws_software_raid.sh
/opt/vertica/sbin/configure_spread
/opt/vertica/sbin/copy_vertica_license
/opt/vertica/sbin/createRootPem
/opt/vertica/sbin/mod_spread
/opt/vertica/sbin/mod_utils
/opt/vertica/sbin/reconfigure_cluster
/opt/vertica/sbin/setup_storage.sh
/opt/vertica/sbin/vconf
```

```
/opt/vertica/sbin/vertica_agent
/opt/vertica/sbin/restart_agent
/opt/vertica/sbin/vertica_agent.service
/opt/vertica/sdk/docker
/opt/vertica/sdk/examples
/opt/vertica/share/CSD
/opt/vertica/share/vbr/example_configs
/opt/vertica/agent
/opt/vertica/agent/samples
```

External procedures and User-defined extensions (UDx) should only be used as necessary. Any required Udx or external procedure should be documented and access to create and execute these functions should be limited to a dbadmin superuser only. To view the user libraries:

SELECT * from user_libraries;

Any libraries that are not documented should be dropped. For details on how to drop the libraries see the **SQL Reference Manual,** https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/SQLReferenceManual/Statements/DROPLIBRARY.htm

Vertica includes optional add-on packages. If any of these packages are not used within the system, the package should be removed. To view the list of available packages, run this command from the host command prompt:

$ admintools -t list_packages

Review the list and determine if any listed packages are not needed by the organization. The Kafka package is required for operations within this document to stream messages to central log server. To remove a package, run this command:

$ admintools -t uninstall_packages -d <*database name*> -p <*dbadmin password*> -P <*name of packages*>

If the packages are needed by the organization, document the usage.

3. SUT Configurations

Once installation is complete, administrators must perform additional configuration steps to ensure Vertica operates in the compliant configuration. These additional configuration steps are described in the sections below.

3.1 Client Authentication

Client connections to Vertica can be one of the following types:

- LOCAL – the dbadmin account must use local hash authentication with the SHA512[12] option. Applications accessing Vertica that reside on the same platform as the database may also use this method.
- HOST – non-DBADMIN users, must use HOST authentication.

For HOST connections there are multiple client authentication options. Whenever possible Vertica should be incorporated into the enterprise authentication for the organization. The following options can be used to achieve STIG compliance:

- LDAP over TLS – this method requires a username and password but uses an LDAP or Active Directory server to verify the password. The CA for the LDAP server is also required. The `ldap.conf` file in the underlying OS should point to the CA certificate folder. The TLS_REQCERT option must be set to 'hard'. For details on these configurations, please see the **Security and Authentication** section, **Client Authentication** section, **LDAP Authentication** section of the Vertica documentation and refer to **Using LDAP Over SSL/TLS** (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/ClientAuth/UsingLDAPOverSSLAndTLS.htm) for configuration steps.
    - LDAPS and not StartTLS should be used.
    - The OpenLDAP client must be installed on RHEL[13] operating system prior to LDAP configuration
    - Multiple LDAP servers can be configured is needed. See https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/ClientAuth/ConfiguringMultipleLDAPServers.htm for details
    - Anonymous binding should not be used.
- Kerberos – this method requires the Kerberos 5 client package installed on each server and client. On RHEL the client can be found in /etc. If necessary, the software can be found at http://web.mit.edu/kerberos/dist/. Each node must have access to a Kerberos Key Distribution Center (KDC).
    - To configure Kerberos on Vertica see https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/Kerberos/ConfigureVerticaForKerberosAuthentication.htm
    - The Active Directory server must also be configured. See https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/Kerberos/CreatingthePrincipalsandKeytabonActiveDirectory.htm for how to configure. Ensure that Password never expires is not checked.

[12] SHA512 – Secure Hash Algorithm with output size 512 bits
[13] RHEL – Red Hat Enterprise Linux

- To configure Vertica clients for Kerberos see https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/Kerberos/ConfigureClientsForKerberosAuthentication.htm
- Run the KERBEROS_CONFIG_CHECK when configurations are complete.

- In addition, it is recommended to set a Reject policy for clients not using TLS. See the **Security and Authentication** section, **Client Authentication** section of the Vertica documentation and refer to the **Creating Authentication Records**. The following command should be run:

  CREATE AUTHENTICATION RejectNoSSL METHOD 'reject' HOST NO TLS '0.0.0.0/0'

3.2 TLS Configuration

Vertica can be configured to use TLS for client/server communications and communications between nodes.

3.2.1 Server Certificate Configuration

When enabling client authentication over TLS for mutual mode, all non-DoD[14] CA shall be removed using:

ALTER DATABASE <*database name*> CLEAR SSLCertificate;
ALTER DATABASE <*database name*> CLEAR SSLPrivateKey;
ALTER DATABASE <*database name*> CLEAR SSLCA;

Obtain certificates issued by the site's CA. The following certificates are needed:

- CA certificate (root.crt),
- Database inter-node server certificate,
- Database inter-node server private key,
- Database server certificate,
- Database server private key,
- Client private key (client.key),
- Client certificate (client.crt).

The inter-node server, server and client certificates must be signed by the CA. To enable client-server TLS the server certificates are loaded onto the system using the following commands:

ALTER DATABASE DEFAULT SET SSLCA = '<*content of CA certificate file*>';
ALTER DATABASE <*database name*> SET SSLCertificate = '<*content of server certificate file* >';
ALTER DATABASE <*database name*> SET SSLPrivateKey = '<*content of server private key*>';

The database must be stopped and restarted for the configuration to take effect.

If the database is in a multi-node cluster, the server.crt and root.crt files will need to be shared to all hosts on the cluster to enable client connections to each host using mutual authentication. The Administration Tools, Configuration Menu can be used to distribute keys. Select the Distribute Config Files and select OK.

[14] DoD – Department of Defense

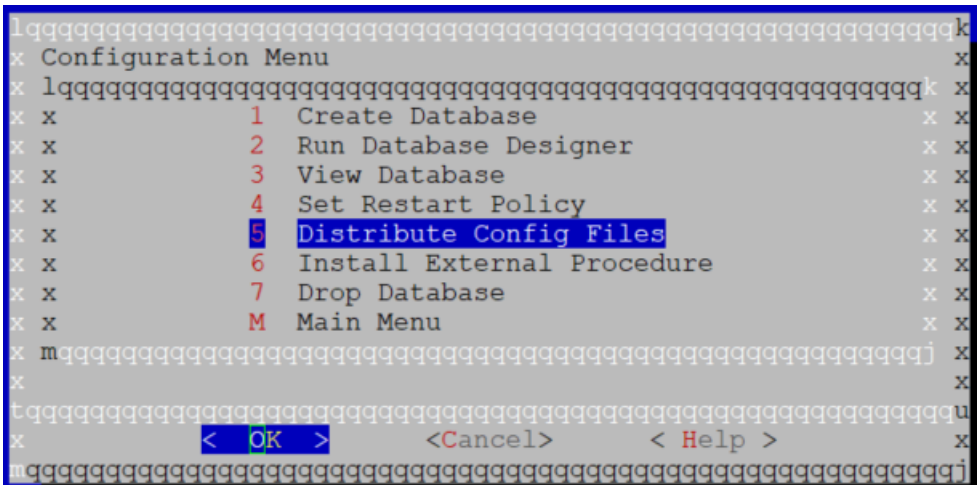

Figure 1 – Administration Tools Configuration Menu

Next select SSL Keys, to distribute the keys and click OK.

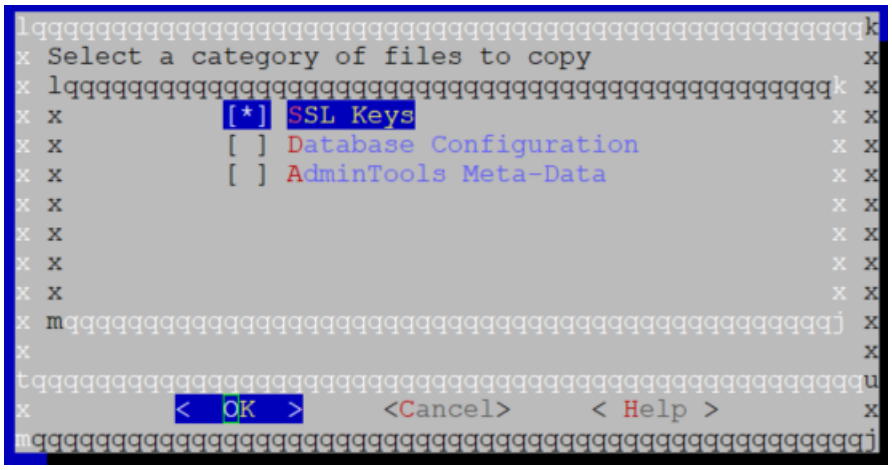

Figure 2 – Administration Tools Distribute Config Files Menu

You will be asked to select the database and will then be presented with the key files to distribute. Both server and CA certificate, as well as the private key should be distributed to all nodes.

3.2.2 Client Authentication over TLS

Once the server certificates have been distributed, client connections should be configured to connect over TLS using mutual authentication. To configure the database to use TLS in Mutual Mode, run:

ALTER DATABASE <*database name*> SET EnableSSL=1;

Refer to **Security and Authentication** section, **TLS/SSL Server Authentication** section, **SSL Authentication** section of the documentation and follow details in the **Setup TLS/SSL Server for Mutual Mode Authentication** section (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/SSL/SSLPrerequisites.htm).

The **Connecting to Vertica** section of the documentation also describes how to enable TLS connections on client drivers. FIPS compatible drivers should be used. Please see https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/ConnectingToVertica/ClientDriverMisc/ClientDriverAndServerVersionCompatibility.htm to determine which drivers to use. The client private key, client certificate, and CA certificate must be accessible to the client applications.

3.2.3 Internode TLS

In general, the connections between database nodes should be on a distinct network that is not connected to any other devices. If it is not possible to connect the nodes in this manner, then Internode TLS should be used to encrypt the control- and data-channels. For details on how to configure this protection, see the **Security and Authentication** section of the documentation, **Internode Communication and Encryption** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/SSL/InternodeSSL.htm).

For the Control Channel, the EncryptSpreadComm parameter should be set to 'vertica' to allow Vertica to generate the encryption key. For example:

```
SELECT SET_CONFIG_PARAMETER('EncryptSpreadComm', 'vertica');
```

The Data Channel uses the DataSSLParams parameter and requires a list of the TLS certificates. The inter-node server certificate and inter-node server private key should be used for this configuration. For example:

```
SELECT SET_CONFIG_PARAMETER('DataSSLParams', '<content of DoD issued inter-node server certificate>, <content of DoD issued inter-node private key>, <content of CA certificate>');
```

3.2.4 Verifying TLS Configurations

Once all TLS configurations are complete, the database should be restarted; then, run the following command:

```
SELECT SECURITY_CONFIG_CHECK ('NETWORK');
```

This command will verify the TLS configurations are set properly and output the configurations for review. A sample of a valid configuration is shown below:

```
Vertica=> SELECT SECURITY_CONFIG_CHECK('NETWORK');

              SECURITY_CONFIG_CHECK

-------------------------------------------------------
-------------------------------------------------------
-----------------------------------------------
 Spread security details:
* EncryptSpreadComm = [vertica]
Spread encryption is enabled
It is now safe to set/change other security knobs

Data Channel security details:
* DataSSLParams is set
SSL on the data channel is enabled

Client-Server network security details:
* EnableSSL is set
* SSLCertificate is set
* SSLPrivateKey is set
Client-Server SSL is enabled

(1 row)
```

Figure 3 – Sample Network Security Configuration Check

3.3 User Configurations

Vertica provides a number of configurations for how users connect to the database. In cases where the database is embedded, the application will likely control access to the database. For stand-alone or cluster configurations, ensure the configurations in the following sections are performed.

3.3.1 Database Roles

Vertica has five pre-defined roles; DBADMIN, PSEUDOSUPERUSER, DBDUSER, SYSMONITOR, and PUBLIC. The DBADMIN role should only be granted to administrators authorized to configure the database and set security controls. All non-DBA users are assigned the PUBLIC role by default. Only the DBADMIN and PSEUDOSUPERUSER can assign users to a role. Assignments should be made carefully to ensure that separation of privileges and least privilege concepts are maintained. To see more about roles and how they are granted, see the **Administrator's Guide**, **Database Users and Privileges** Section, **Database Roles** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/DBUsersAndPrivileges/Roles/AboutDatabaseRoles.htm).

During database installation, a database owner user is created. By default, this user is named dbadmin. The dbadmin username can change, but there must be one database owner. This database owner has the superuser privilege. Vertica superusers have complete and irrevocable authority over database users, privileges, and roles. This dbadmin is not the same as the DBADMIN role discussed above. Throughout this document, this user will be referred to as dbadmin.

3.3.2 Limit number of concurrent sessions

The database must limit the number of concurrent sessions a user can have to an organization defined number (SRG-APP-000001-DB-000031). Use the following command for this setting:

ALTER USER <*username*> MAXCONNECTIONS <*organization defined number*> on DATABASE;

This setting must be configured for each user on the system. The dbadmin user is the only user authorized to change MAXCONNECTIONS.

3.3.3 Set session idle timeout

Timeouts shall be configured at 15 minutes for users, and 10 minutes for administrators. To set a default idle timeout for all users, use the following command:

ALTER DATABASE DEFAULT SET defaultidlesessiontimeout = '900 secs';

Individual user timeouts should only be more restrictive than this limit. To set a default idle timeout of 10 minutes for all administrators, use the following:

ALTER USER <username> IDELSESSSIONTIMEOUT '600 secs' on DATABASE;

3.3.4 Password configurations

While LDAP is the preferred method for authentication, passwords will also need to be used. To ensure proper security when password-based authentication is used, use the Profile to set the password requirements. Either ALTER DEFAULT or CREATE can be used for these commands:

CREATE PROFILE <*profile-name*> LIMIT PASSWORD_MIN_LENGTH 15;
CREATE PROFILE <*profile-name*> LIMIT PASSWORD_MIN_LOWERCASE_LETTERS 1;
CREATE PROFILE <*profile-name*> LIMIT PASSWORD_MIN_UPPERCASE_LETTERS 1;
CREATE PROFILE <*profile-name*> LIMIT PASSWORD_MIN_DIGITS 1;
CREATE PROFILE <*profile-name*> LIMIT PASSWORD_MIN_SYMBOLS 1;
CREATE PROFILE <*profile-name*> LIMIT PASSWORD_REUSE_MAX 5;
CREATE PROFILE <*profile-name*> LIMIT PASSWORD_LIFE_TIME 60;

Next, assign the profile to users and expire the old password. This ensures these rules are immediately applied to users. To ensure that passwords are stored in a secure manner, change the Security_Algorithm used to SHA-512 with the following:

ALTER DATABASE DEFAULT SET Security_Algorithm = 'SHA512'

3.4 Database Access

Vertica uses profiles to control the level of access for which each user is authorized. The following configurations should be made.

3.4.1 Minimum access requirements

All new users are automatically assigned the PUBLIC role. This role controls the minimum access requirements to the database. By default, the USAGE privilege is assigned, but additional privileges can be granted by the dbamin user. Only assign privileges to this role that are required for all users.

For a list of privileges needed for every action on the database, see the **Administrator's Guide**, Section **Database Users and Privileges,** Section **Database Privileges,** Section **Privileges Required for Common Database Operations**. (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/DBUsersAndPrivileges/Privileges/PrivilegesRequiredForCommonDatabaseOperations.htm).

3.4.2 Access to system tables

Vertica includes a set of system tables that monitor the database itself. To see the list of system tables and their contents, see (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/SQLReferenceManual/SystemTables/VerticaSystemTables.htm) within the SQL Reference Manual.

Administrators should avoid granting access to system tables beyond those necessary for a given user to perform their duties. To view which system tables are accessible to the PUBLIC role, use the following:

```
SELECT * FROM grants WHERE grantee='public';
```

For any system tables that should not be universally accessible, use the following to revoke access from PUBLIC:

```
REVOKE ALL ON <table name> from <user/role>;
```

Certain system tables are marked as monitorable. The SYSMONITOR role has irrevocable access to all system tables marked "monitorable". Users with PSEUDOSUPERUSER role have irrevocable access to all system tables. Grant these roles only when necessary.

3.4.3 Monitoring User Privileges

The AUDIT_MANAGING_USERS_PRIVILEGES table provides a summary of information about changes to privileges, user management and authentication changes. To see what data can be obtained from the tables see (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/SQLReferenceManual/SystemTables/CATALOG/AUDIT_MANAGING_USERS_PRIVILEGES.htm) within the **SQL Reference Manual**.

This table can provide the following information on changes to users and user's privileges:

- Privileges added – using a GRANT statement
- Privileges removed – using a REVOKE statement
- Users created – using a CREATE USER statement

Additionally, this tables shows when queries on user privileges have occurred for tables GRANTS, USERS, PROFILES, CLIENT_AUTH, ACCESS_POLICY.

3.4.4 Using Schemas for Security Levels

If a database contains classified data, it is vital to restrict access to data according to the classification of the data. Creating different schemas for each classification/security level is an effective way to ensure separation of this data. See the **Administrator's Guide** documentation, **Configuring the Database** section, **Designing a Logical Schema** section, **Multiple Schemas** section, **Multiple Schema Examples** page for details on how to create multiple schemas (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/ConfiguringTheDB/LogicalSchema/MultipleSchemaExamples.htm).

3.5 Auditing Configurations

Vertica database maintains verbose data that can be used for auditing. Documentation on auditing can be found in the **Administrator's Guide** documentation, **Monitoring Vertica** section. The main sources of this data are:

- *Vertica.log* – This file is maintained for each node in the data. It is a running log of all activities on that node. This file can be rotated with maximum size limits set. For more details on *vertica.log,* see the **Monitoring Log File** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Monitoring/Vertica/MonitoringLogFiles.htm).
- *dbLog* – This file collects events during system start-up before *vertica.log* is started.
- System tables – there are two schemas of system tables:
  - V_CATALOG: Provides information about persistent objects in the database
  - V_MONITOR: Provides information about transient system state

  The system tables store information on privileges, queries that have been run, and database state information. They can be queried like any other table within the database. For more details, see the **Using System Tables** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Monitoring/Vertica/UsingSystemTables.htm).
- Data Collector – A set of tables that collects data from system tables across all nodes of a database.
- Syslog – The syslog configuration for the database pertains only to SNMP messages that can be sent to a centralized audit server. None of the other audit data listed above is included in the syslog functions.

Vertica.log and Data Collector tables can be sent to a centralized audit server. System tables cannot be directly sent to a centralized audit server. Each site should determine which files to send to the audit server. In general, for an embedded system, the *vertica.log* file is sufficient to meet SRG requirements. For a clustered database, Data Collector tables should be used to cover all nodes within the cluster. Details on how to configure sending each of these to a centralized audit server are provided below.

Table 2 provides an overview of the audit events required by the Database SRG and how the data can be obtained within Vertica.

Table 2 – Database SRG Audit Events in Vertica

Log Requirement	Search Command	Vertica.log	Notes
• Successful login • Start and end time for user access to the systems SRG-APP-000492-DB-000333 SRG-APP-000505-DB-000352 SRG-APP-000506-DB-000353	SELECT * from USER_SESSIONS;	Yes	For stand-alone or clustered systems this table will also show concurrent logins from different workstations.
Unsuccessful login SRG-APP-000503-DB-000351	SELECT * from LOGIN_FAILURES;	Yes	
Successful permission grants SRG-APP-000495-DB-000326	SELECT * from GRANTS;	Yes	Can further specify privileges_description (SELECT, EXECUTE, USAGE) Grantee (a specific username)

Log Requirement	Search Command	Vertica.log	Notes
Successful and unsuccessful creation, modification, or deletion of users, roles or privileges SRG-APP-000495-DB-000327 SRG-APP-000495-DB-000328 SRG-APP-000495-DB-000329 SRG-APP-000499-DB-000330 SRG-APP-000499-DB-000331	SELECT * from AUDIT_MANAGING_USERS_PRIVILEGES	Yes	The column 'success' will be listed as 't' for true and 'f' for false. [To use a dc table: SELECT * from dc_request_issued where request_type ilike 'DDL'; Then search for CREATE, ALTER, DELETE]
Unsuccessful requests within the database. SRG-APP-000091-DB-000325 SRG-APP-000496-DV-000335 SRG-APP-000501-DB-000337 SRG-APP-000494-DB-000345 SRG-APP-000498-DB-000347 SRG-APP-000502-DB-000349	SELECT * from dc_requests_completed WHERE SUCCESS='f'	Yes	This will show all failed requests.
View when queries are performed to view privileges on the database SRG-APP-000091-DB-000066	SELECT * from LOG_TABLES where CATEGORY ilike 'Managing_Users_Privileges'	Yes	
Enforcement of access restrictions SRG-APP-000381-DB-000361	None	Yes	Failed requests are logged, with their associated reason for failure in *vertica.log*. Reason for failure is listed in ERROR event.
Successful access to system tables or any tables deemed a security object. SRG-APP-000492-DB-000333 SRG-APP-000496-DB-000334 SRG-APP-000501-DB-000336	SELECT * from LOG_TABLES where CATEGORY ilike 'Security'	Yes	Can also use dc_requests_completed table and search for a particular table with a command_tag or SELECT, INSERT, UPDATE, DELETE, or EXECUTE.
Successful access, modification, deletion of security levels (separate schemas) SRG-APP-000494-DB-000344 SRG-APP-000498-DB-000346 SRG-APP-000502-DB-000348	SELECT * from dc_requests_completed	Yes	Each command_tag would need to be searched separately: Create Schema, ALTER Schema, DELETE Schema
All privileged activities SRG-APP-000504-DB-000354	SELECT * from dc_requests_issued where request_type ilike 'DDL'	Yes	
All object access SRG-APP-000507-DB-000356	SELECT * from dc_requests_completed	Yes	Each of the following command_tags would need to be searched: CREATE, ALTER, DROP, REVOKE, DENY GRANT statements can be using the GRANTs table.

Log Requirement	Search Command	Vertica.log	Notes
All session starts and session ends SRG-APP-000505-DB-000352	SELECT * from dc_session_starts WHERE is_interal='f'; SELECT * from dc_session_ends WHERE session_id='*<session ID from session start>*';	Yes	It is recommended to run the session starts command and then use the session ID to check for session end.

3.5.1 Sending Log Files

The underlying operating system can be used to send *vertica.log* files to a centralized audit server. There are numerous log collectors that can be used for this purpose. Examples of these include:

- Logstash (https://www.elastic.co/logstash) – The logstash file plugin in tail mode can be used to send changes to the *vertica.log* file to a configured centralized audit server.
- Elastic (https://www.elastic.co/log-monitoring) – The ELK Stack uses Beats to ship data to centralized audit servers. The filebeat can be used to send *vertica.log* files to a configured centralized audit server or can be integrated with Logstash.

These modules are independent of the Vertica database. Any database deployed on a Linux-based operating system can use these modules to integrate implicit Vertica auditing with the underlying operating system auditing. The *vertica.log* file is unique per node, so each node would need to be configured to send these messages to the centralized log server. Events are annotated with the node name unless they are database events. Events with the level of LOG, QUERY, TXN, ERROR, and FATAL should be sent to the centralized audit server.

3.5.2 Vertica Notifiers

Notifiers can be configured to send changes to Data Collector tables as messages to an Apache Kafka server. The Kafka server can then send queued messages to the site's centralized audit server. Instructions for creating notifiers and sending Data Collector table updates to Kafka can be found in the **Administrator's Guide** section of the Vertica documentation, **Monitoring Vertica** section and **Monitoring Vertica Using Notifiers** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Monitoring/Vertica/MonitoringUsingNotifiers.htm). Notifiers aggregate audit data across multiple nodes, supporting their use for clustered deployments.

Notifiers must be created, using CREATE NOTIFIER, to send messages to the Apache Kafka server. Configure the MAXMEMORYSIZE and Kafka-related PARAMETERS to ensure messages are not frequently dropped.

> CREATE NOTIFIER vertica_logs ACTION 'kafka : //*<Kafka server address:port number>*' MAXMEMORYSIZE '10M';

Once the notifier has been created, use the SET_DATA_COLLECTOR_NOTIFY_POLICY command to send Data Collector tables to the Kafka server. For more details see the example in the **Data Collector Functions** (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/SQLReferenceManual/Functions/VerticaFunctions/DataCollection/SET_DATA_COLLECTOR_NOTIFY_POLICY.htm).

3.5.3 Data Collector

The Data Collector component is enabled by default. The current Data Collector policies can be viewed using the command:

```
SELECT * from data_collector;
```

Retention policies can be configured for data as needed. The following Data Collector tables are needed to meet SRG requirements:

- dc_configuration_changes – shows all changes made to the *vertica.conf* file
- dc_login_failures – shows failed login attempts
- dc_notifier_errors – shows errors in the notifier functionality
- dc_requests_issued – a comparison of requests issued to requests completed can show failed requests and failed access attempts
- dc_requests_completed – a comparison of requests issued to requests completed can show failed requests and failed access attempts
- dc_session_starts – shows the start of all sessions to the database
- dc_session_ends – shows the end of all sessions to the database

An example of setting the notifier for the Configuration Changes table is:

```
SELECT SET_DATA_COLLECTOR_NOTIFY_POLICY('configurationchanges', 'vertica_logs',
'vertica_notifications', true);
```

A notifier should be added for each of the Data Collector tables listed above.

3.5.4 Syslog Configuration

Enabling syslog allows logs to be sent to the underlying operating system in `/var/log/messages` for each host system. This, then allows the logs to be sent to a centralize syslog server. Different than the notifiers discussed above, these logs are cover events such as:

- Low Disk Space
- Loss of K Safety
- Current Fault Tolerance at Critical Level
- Recovery Failure
- Recovery Error

Configurations for syslog can be found in the **Administrator's Guide** documentation, **Monitoring Vertica** section, **Monitoring Events** section, **Configuring Event Reporting** section, on the **Configuring Reporting for Syslog** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Monitoring/Vertica/ConfiguringReportingForSyslog.htm). An example of the configurations is:

```
ALTER DATABASE DEFAULT SET SyslogEnabled = 1;
ALTER DATABASE DEFAULT SET SyslogEvents = 'Low Disk Space, Loss of K Safety';
```

Administrators should ensure that the configured list of events matches those defined by the organizational needs. The Low Disk Space event must be included to meet SRG-APP-000359-DB-000319.

3.5.5 Log Rotation Policies

The operating system's log rotate function can be used to rotate the *vertica.log* file. The storage location of this file can be configured during installation. By default, the log file is stored in the `catalog-path/database-name/node-name` directory. To view the log file use the following command:

```
$ tail -f catalog-path/database-name/node-name/vertica.log
```

The Administration Tools includes a logrotate utility that allows the administrator to set how often logs are rotated, the maximum file size for logs and how long to keep logs. This employs scripts to configure the logrotate function present in the underlying OS. For more details, see the **Administrator's Guide** documentation, **Monitoring Vertica** section, **Rotating Log File** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Monitoring/Vertica/RotatingLogFiles.htm). This meets SRG-APP-000357-DB-000316 and SRG-APP-000109-DB-000321.

Data Collector tables need to have retention policies set. These retention policies determine how much data is retained and for how long. The following commands will show the current retention policies:

```
SELECT get_data_collector_policy('ResourceAcquisitions');
SELECT get_data_collector_policy('RequestsIssued');
```

These policies should be set to ensure minimal loss of audit data. See the **Administrator's Guide** documentation, **Monitoring Vertica** section, **Retaining Monitoring Information** section, **Configuring Data Retention Policies** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Monitoring/Vertica/ConfiguringDataRetentionPolicies.htm) for details on how to configure appropriate policies.

3.5.6 Time stamps

Vertica uses the system time, but the timezone can be configured as required by each organization. To set the timezone use:

```
SET TIMEZONE TO <name of time zone>;
```

The list of supported time zones can be found in `/opt/vertica/share/timezonesets`. This meets the SRG-APP-000374-DB-00322.

3.6 Requirements Mapping

This section maps the Database SRG STIG ID to the appropriate response. The embedded database is the most common deployment type seeking being STIG tested. There is a column covering embedded database responses and a separate column for stand-along or clustered database deployments. The responses refer to the above section for more details where appropriate.

Table 3 – Mapping of Database SRG STIG IDs to Vertica Deployment Types

STIG ID	Embedded Database Response	Stand-alone or cluster database response
SRG-APP-000001-DB-000031	The application should manage concurrent session limits.	See Section 3.3.2 Limit number of concurrent sessions.
SRG-APP-000023-DB-000001	The application will likely manage accounts.	See Section 3.1 Client Authentication – LDAP or Kerberos.
SRG-APP-000033-DB-000084	This requirement is met with a combination of roles and privileges per site policies. See Section 3.3.1 Database Roles and 3.4.1 Minimum Access Requirements. Configured roles and privileges are always enforced by the database. Restricting access to system tables should also be configured. See 3.4.2 Access to system tables.	This requirement is met with a combination of roles and privileges per site policies. See Section 3.3.1 Database Roles and 3.4.1 Minimum Access Requirements. Configured roles and privileges are always enforced by the database. Restricting access to system tables should also be configured. See 3.4.2 Access to system tables.
SRG-APP-000089-DB-000064	See Table 2 for how to find specific audit events.	See Table 2 for how to find specific audit events.
SRG-APP-000091-DB-000066	See Table 2 for view when queries are performed to view privileges on the database	See Table 2 for view when queries are performed to view privileges on the database
SRG-APP-000091-DB-000325	See Table 2 for unsuccessful requests. This includes all unsuccessful requests.	See Table 2 for unsuccessful requests. This includes all unsuccessful requests.
SRG-APP-000101-DB-000044	Requires site information on additional audit information that is required. Data Collector (3.5.3) should be able to support requirements.	Requires site information on additional audit information that is required. Data Collector (3.5.3) should be able to support requirements.
SRG-APP-000109-DB-000049	Not applicable due to availability requirements. Must enable sending vertica.log or Data Collector tables changes to a central audit server: 3.5 Must enable log rotation: 3.5.5 Log Rotation	Not Applicable due to availability requirements. Must enable sending Data Collector tables changes to a central audit server: 3.5 Must enable log rotation: 3.5.5 Log Rotation
SRG-APP-000133-DB-000200	CREATE privileges should be limited to dbadmin user or the application user if required.	Assign users CREATE privileges as required per site policy.
SRG-APP-000133-DB-000362	If no access is provided to change the database structure, this check is not applicable.	Ensure that only administrators designated by the site as assigned the DBADMIN role. See 3.3.1 Database Roles.
SRG-APP-000141-DB-000090 SRG-APP-000141-DB-000091 SRG-APP-000141-DB-000092 SRG-APP-000243-DB-000128	Remove sample databases and unused components: 2.1 Additions to Initial Configuration To confirm that No data from development or testing remains in the database. To confirm this, query SELECT * from schemata where is_system_schema = ‘f’; and show that none exist.	Remove sample databases and unused components: 2.1 Additions to Initial Configuration To confirm that No data from development or testing remains in the database. To confirm this, query SELECT * from schemata where is_system_schema = ‘f’; and show that none exist.
SRG-APP-000142-DB-000094 SRG-APP-000383-DB-000364	Disable any ports not listed in 1.6 or needed by application	Disable any ports not listed in 1.6

STIG ID	Embedded Database Response	Stand-alone or cluster database response
SRG-APP-000148-DB-000103 SRG-APP-000180-DB-000115	Not applicable. The application is the only user of the database and therefore organizational users do not exist.	Not applicable. Each user is uniquely identified. These users may be assigned permissions as a group, but all individuals are uniquely identified on the database.
SRG-APP-000171-DB-000074	Configure passwords to be stored using SHA-512: 3.3.4	Configure passwords to be stored using SHA-512: 3.3.4
SRG-APP-000172-DB-00075	Not applicable. Passwords are used internally, but not over a network connection.	Enable Mutual TLS for client connections: Section 3.2.2 Client Authentication over TLS Use LDAP over TLS: 3.1 Client Authentication
SRG-APP-000175-DB-000067 SRG-APP-000176-DB-000068	Not applicable. Users may use PKI-based authentication to authenticate to the application, but since the application and database reside on the same host, PKI-based authentication is not necessary.	Users can use LDAP authentication to support PKI-based authentication. The LDAP server will then be required to meet RFC 5280 requirements for certificate-based authentication.
SRG-APP-000177-DB-000069	The application should perform certificate-based authentication. This requirement is Not Applicable. The application can perform password-based authentication to the database.	Enable Mutual SSL for client connections along with use of LDAP. See Sections 3.2.2 Client Authentication over TLS and 3.1 Client Authentication
SRG-APP-000179-DB-000114 SRG-APP-000416-DB-000380 SRG-APP-000514-DB-000381 SRG-APP-000514-DB-000382 SRG-APP-000514-DB-000383	Vertica relies on the underlying OS to provide a FIPS validated library. RHEL 8 is In Review for FIPS validation. Vertica v9.2.x includes FIPS validated module when operated on RHEL 6.6.	Vertica relies on the underlying OS to provide a FIPS validated library. RHEL 8 is In Review for FIPS validation. Vertica v9.2.x includes FIPS validated module when operated on RHEL 6.6.
SRG-APP-000225-DB-000153	When the database is restarted it will ask to use the Last Good Epoch.	If a node failed, but the cluster continued to operate, the node will be automatically recovered, and data will be synced with other nodes before the node is back online. If failures resulted in the cluster shutting down, the database will ask to use the Last Good Epoch.
SRG-APP-000231-DB-000154	Not Applicable unless required by site If required use self-encrypting drives for storage	Not Applicable unless required by site If required use self-encrypting drives for storage
SRG-APP-000233-DB-000124	Users, roles, privileges and audit settings are all stored in distinct tables with permission levels. User data is not stored in these tables. Separate schemas can be created to more fully separate these functions if necessary.	Users, roles, privileges and audit settings are all stored in distinct tables with permission levels. User data is not stored in these tables. Separate schemas can be created to more fully separate these functions if necessary.

STIG ID	Embedded Database Response	Stand-alone or cluster database response
SRG-APP-000243-DB-000373	This check is not applicable for an embedded database since there is only one user of the database, the application.	Vertica protects against unintentional information transfer via shared resources using database locks and isolation levels. See for details on how to set isolation levels https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/ConceptsGuide/Other/Transactions.htm Temporary tables are not accessible to other sessions. https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/Tables/CreatingTemporaryTables.htm
sweetSRG-APP-000342-DB-000302	If user functions are used provide a list of user functions and details on when and why they are needed. If no user functions are used, this check is not applicable.	If user functions are used provide a list of user functions and details on when and why they are needed. If no user functions are used, this check is not applicable.
SRG-APP-000295-DB-000305	See Section 3.3.3 to configured session timeouts.	See Section 3.3.3 to configured session timeouts.
SRG-APP-000311-DB-000308 SRG-APP-000313-DB-000309 SRG-APP-000314-DB-000310	Security labeling may not be required at site. In this case, this check would be Not Applicable. If security labeling is required, this can be accomplished with schemas for different levels of classification and data access controls on the data. These controls would remain in place during storage and preparation. The application should ensure that reports are designed to mark data with classifications and that security labels are maintained during transmission.	Security labeling may not be required at site. In this case, this check would be Not Applicable. If security labeling is required, this can be accomplished with schemas for different levels of classification and data access controls on the data. These controls would remain in place during storage, preparation, and transmission.
SRG-APP-000353-DB-000324 SRG-APP-000090-DB-000065	The dbamin can set what Data Collector tables are sent to centralized server 3.5.3.	The dbadmin can set what Data Collector tables are sent to centralized server 3.5.3
SRG-APP-000356-DB-000314 SRG-APP-000356-DB-000315 SRG-APP-000515-DB-000318	Must enable sending to a centralized audit server using Kafka: 3.5.2 For embedded systems sending with application logs may be appropriate, see Section 3.5.1.	Must enable sending to a centralized audit server using Kafka: 3.5.2 or *vertica.log: 3.5.1*
SRG-APP-000357-DB-000316 SRG-APP-000109-DB-000321	Must enable log rotation using the MaxFileSize: 3.5.5 Log Rotation for *vertica.log.* See also 3.5.5 for details on retention policies for Data Collector.	Must enable log rotation using the MaxFileSize: 3.5.5 Log Rotation for *vertica.log.* See also 3.5.5 for details on retention policies for Data Collector.
SRG-APP-000359-DB-000319	Configure syslog with low disk space event, see Section 3.5.4.	Configure syslog with low disk space event, see Section 3.5.4.

STIG ID	Embedded Database Response	Stand-alone or cluster database response
SRG-APP-000360-DB-000320	The centralize audit server can be used to provide alerts of audit failures. Vertica database does not need to provide these alerts.	The centralize audit server can be used to provide alerts of audit failures. Vertica database does not need to provide these alerts.
SRG-APP-000374-DB-000322	Configure the appropriate timezone: 3.5.6	Configure the appropriate timezone: 3.5.6
SRG-APP-000381-DB-000361	See Table 2 for enforcement of access restrictions.	See Table 2 for enforcement of access restrictions.
SRG-APP-000389-DB-000372	Not applicable for embedded databases the application is the only user.	While this requirement is not met automatically by the system, it can be met through administrator policy to use: ALTER <*username*> PASSWORD EXPIRE After performing any of the following actions: i. Type of authentication changes ii. User's role changes The other circumstances listed in the requirement: iii. Not applicable unless database includes a mixed classification environment. iv. Database does not allow escalation of privileges. v. See Timeout configurations in 3.3.3
SRG-APP-000454-DB-000389	Software that has been replaced or made unnecessary by an update is automatically removed as part of the update process. To confirm view the installation files in `/opt/vertica` and ensure that no unused software is present.	Software that has been replaced or made unnecessary by an update is automatically removed as part of the update process. To confirm view the installation files in `/opt/vertica` and ensure that no unused software is present.
SRG-APP-000495-DB-000326 SRG-APP-000495-DB-000327 SRG-APP-000495-DB-000328 SRG-APP-000495-DB-000329 SRG-APP-000499-DB-000330 SRG-APP-000499-DB-000331	Use AUDIT_MANAGING_USER_PRIVILEGES to monitor changes to user privileges : 3.4.2 Monitoring User Privileges See Table 2 on Successful and unsuccessful creation, modification, or deletion of users, roles or privileges.	Use AUDIT_MANAGING_USER_PRIVILEGES to monitor changes to user privileges : 3.4.2 Monitoring User Privileges See Table 2 on Successful and unsuccessful creation, modification
SRG-APP-000494-DB-000344 SRG-APP-000494-DB-000345 SRG-APP-000498-DB-000346 SRG-APP-000498-DB-000347 SRG-APP-000502-DB-000348 SRG-APP-000502-DB-000349	If the database does not include classified data, this check is not applicable. If there is classified data, separate schemas are required for different levels of data. See Table 2 Access to security levels for details on audit events.	If the database does not include classified data, this check is not applicable. If there is classified data, separate schemas are required for different levels of data. See Table 2 Access to security levels for details on audit events.
SRG-APP-000496-DB-000334 SRG-APP-000507-DB-000356 SRG-APP-000507-DB-000357	See Table 2 Object access.	See Table 2 Object access.

STIG ID	Embedded Database Response	Stand-alone or cluster database response
SRG-APP-000492-DB-000332 SRG-APP-000492-DB-000333 SRG-APP-000496-DB-000334 SRG-APP-000496-DB-000335 SRG-APP-000501-DB-000336 SRG-APP-000501-DB-000337	For each product the vendor will need to determine what the security objects are. Those tables and/or schemas are then protected with access policies. For embedded systems, it may be that these security configurations cannot be changed. If so, this check is not applicable.	For each product the vendor will need to determine what the security objects are. Those tables and/or schemas are then protected with access policies. Auditing of access to these tables and schemas will be performed by dc_requests_issued and can be searched by the table or schema that has been identified as a security object and the action (SELECT, INSERT, UPDATE, DELETE, EXECUTE) or failed.
SRG-APP-000503-DB-000350 SRG-APP-000503-DB-000352 SRG-APP-000506-DB-000353	See Table 2 Successful Login.	See Table 2 Successful Login.
SRG-APP-000503-DB-000351	See Table 2 unsuccessful login.	See Table 2 unsuccessful login.
SRG-APP-000504-DB-000354 SRG-APP-000504-DB-000355	See Table 2 all privileged activities.	See Table 2 all privileged activities.
SRG-APP-000505-DB000352	Use Data Collector dc_session_starts and dc_session_ends to find these records.	Use Data Collector dc_session_starts and dc_session_ends to find these records.
SRG-APP-000514-DB-000383 SRG-APP-000428-DB-000386 SRG-APP-000429-DB-000387	Can state it is Not Applicable if site is not storing information that requires confidentiality. If confidentiality of data is required, self-encrypting drives should be used.	Can state it is Not Applicable if site is not storing information that requires confidentiality. If confidentiality of data is required, self-encrypting drives should be used.
SRG-APP-000508-DB-000358	Not Applicable for embedded systems since access occurs through the application	See Table 2, Session starts.
SRG-APP-000224-DB-000384	This check is not applicable for embedded databases since session hijacking is not possible.	Man-in-the-middle attacks are mitigated through the use of TLS for client communications. See 3.2.2 Client Authentication over TLS.
SRG-APP-000427-DB-000385	This would typically be handled at the application level.	User PKI-based authentication will be handled by the LDAP server. See 3.1 Client Authentication.
SRG-APP-000441-DB-000378 SRG-APP-000442-DB-000379	This requirement is not applicable if data does not require strict data integrity and confidentiality. Data integrity is assured through database locks and confidentiality is ensured through use of secure protocols. See 3.2.2 Client Authentication over TLS.	This requirement is not applicable if data does not require strict data integrity and confidentiality. Data integrity is assured through database locks and confidentiality is ensured through use of secure protocols. See 3.2.2 Client Authentication over TLS, as well as 3.2.3 Internode TLS for clustered databases.
SRG-APP-000251-DB-000391 SRG-APP-000251-DB-000392	Not applicable. By default, dynamic code execution is not allowed.	Not applicable. By default, dynamic code execution is not allowed.

STIG ID	Embedded Database Response	Stand-alone or cluster database response
SRG-APP-000164-DB-000401	Set password policy: 3.3.4 Password configurations	Set password policy: 3.3.4 Password configurations

Table 4 –Database SRG STIG IDs that are Inherently Met by Vertica

STIG ID	Confirmation
SRG-APP-000080-DB-000063 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-000375-DB-000323	All log events include a timestamp, the type of event and the username (if a user-initiated action). Navigate to *vertica.log* and view events to demonstrate the timestamp, type of event and username.
SRG-APP-000092-DB-000208	Monitor *vertica.log* on one system and restart the database on a different system. Ensure that logging begins when the system is started. *dbLog* (catalog path/database name) includes logs that occur before *vertica.log* starts.
SRG-APP-000116-DB-000057	The database must be configured during installation to use system time. For a Red Hat or CentOS system, the system time configuration can be checked with the following command from the CLI: `$ chronyc tracking`
SRG-APP-000118-DB-000059 SRG-APP-000119-DB-000060 SRG-APP-000120-DB-000061	Logs are maintained in *vertica.log* and *dblog*. From the underlying OS, navigate to the `/opt/vertica` folder and view file permissions for *vertica.log* and *dblog*. Ensure that they are set to 0640 or less permissive. Data Collector tables can also be considered logs. From the underlying OS, navigate to the database's catalog directory. Ensure they are set to 0600 or less permissive.
SRG-APP-000121-DB-000202 SRG-APP-000122-DB-000203 SRG-APP-000123-DB-000204	The commands and tools used to manage logs are restricted to the dbadmin user. See Data Collector Functions https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/SQLReferenceManual/Functions/VerticaFunctions/DataCollection/DataCollectorFunctions.htm
SRG-APP-000133-DB-000199	Vertica is installed by default in /opt/vertica/*, while other folders can be used, administrators must keep this folder separate from the host OS and other applications.
SRG-APP-000133-DB-000198 SRG-APP-000133-DB-000179 SRG-APP-000378-DB-000365	Installation of software and software packages is restricted to dbadmin and an OS user with root permissions.
SRG-APP-000141-DB-000093	Access to external executables are restricted to the dbadmin user with superuser privileges to create and those with Schema: USAGE and Procedure: EXECUTE by default. See **Administrator's Guide, Database Users and Privileges** section, **Privileges Required for Common Database Operations** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/DBUsersAndPrivileges/Privileges/PrivilegesRequiredForCommonDatabaseOperations.htm) for details.
SRG-APP-000178-DB-000083	Can be verified by demonstration. No password is displayed when entered.

STIG ID	Confirmation
SRG-APP-000176-DB-000068	Only dbadmin has access to private keys. This can be confirmed by querying the system table. Example: dbadmin=> select current_value from vs_configuration_parameters where parameter_name ilike '%SSL%'; current_value --- <will show value of key>. Create user foo \c – foo foo=> select current_value from vs_configuration_parameters where parameter_name ilike '%SSL%'; current_value --- ******** ← data is masked
SRG-APP-000211-DB-000122	Database user and administrator functionality is separated through the use of roles and privileges. See the **Administrator's Guide, Database Users and Privileges** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/DBUsersAndPrivileges/ManagingUsersAndPrivileges.htm) for more details.
SRG-APP-000220-DB-000149 SRG-APP-000223-DB-000168	Not Applicable for embedded systems Met by default for stand-alone and clustered systems.
SRG-APP-000226-DB-000147	Failure logs can be found in either *vertica.log* or *dbLog*. The database also saves a Last Good Epoch to rollback to, if necessary. See 3.5 for descriptions of *dbLog* and *vertica.log*
SRG-APP-000243-DB-000374	The operating system file permissions are set by default to prevent unauthorized access. This can be verified by confirming the file permission on the database through `/data/vertica/<database name>` and log files and backup files `/opt/vertica` permission. The dbadmin account should own these files and access should be restricted to dbadmin.
SRG-APP-000251-DB-000160	Vertica uses defined and documented APIs and ensures that SQL standards are followed for all inputs.
SRG-APP-000266-DB-000162 SRG-APP-000267-DB-000163	Warning message do not include sensitive data. Details on warning messages can be found at: https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/ErrorCodes/SQLStates.htm
SRG-APP-000328-DB-000301	Discretionary access control policies are always enforced. See **Administrator's Guide**, Section **Database Users and Privileges, Database Privileges, Granting and Revoking** page (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/DBUsersAndPrivileges/Privileges/GrantingAndRevokingPrivileges.htm) for details on GRANT statements and **Access Policies and Query Optimization** (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/AdministratorsGuide/DBUsersAndPrivileges/AccessPolicies/QueryOptimization.htm) for details on column and row access policies.
SRG-APP-000340-DB-000304 SRG-APP-000380-DB-000360 SRG-APP-000516-DB-000363	Non-privileged users inherently do not have permissions to execute privileged functions. The AUDIT_MANAGING_USER_PRIVILEGES table can show privileges within the system. Details on privileges can be seen in section 3.4.1.
SRG-APP-000296-DB-000306	This requirement can be shown by demonstration. Start a session with the database and then logout. Users can type \q to quit and end their database session.
SRG-APP-000400-DB-000367	Cached authenticators must be removed after a defined time period. Cached authenticators are used when Kerberos is enabled. The `kdestroy` command must be included in the logout command to ensure tickets are destroyed.

STIG ID	Confirmation
SRG-APP-000431-DB-000388	If temporary tables are created, they are not visible to other sessions. Vertica employs isolation levels, of which READ COMMITTED is the default. SERIALIZABLE Isolation can also be used. Isolation levels can be set per transaction. Vertica internal processes always run at the SERIALIZABLE isolation level. In both of these isolation levels session isolation is ensured.
SRG-APP-000447-DB-000393	The Vertica database uses defined APIs and SQL standards. Inputs are checked to ensure the SQL standards are met.

The following requirements are the responsibility of the site. While Vertica supports the functionality required to perform these functions, the site must ensure they are accomplished according to the requirement:

- SRG-APP-000456-DB-000390 – Security relevant software updates to the DBMS must be installed within the time period directed by an authoritative source.

  Vertica provides regular updates and notifies customers of the updates. It is a site responsibility to perform the updates in a timely manner.

4. Acronyms

This section defines the acronyms used throughout this document.

Table 5 – Acronyms

Acronym	Definition
APL	Approved Products List
CA	Certificate Authority
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	Department of Defense Information Network
FIPS	Federal Information Processing Standard
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISSM	Information System Security Manager
KDC	Key Distribution Center
LDAP	Lightweight Directory Access Protocol
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
PPSM	Ports, Protocols, and Services Management
RAE	Required Ancillary Equipment
RME	Risk Management Executive
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SRG	Security Requirements Guide
SSH	Secure Shell
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UDx	User-defined Extensions
VLAN	Virtual Local Area Network

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com