23

Strong Authentication Administration Tools

You can use a set of strong authentication administration tools for native network encryption and public key infrastructure credentials.

- About the Configuration and Administration Tools
  The configuration and administration tools manage the encryption, integrity (checksumming), and strong authentication methods for Oracle Net Services.
- Native Network Encryption and Strong Authentication Configuration Tools
  Oracle Net Services can encrypt data using standard encryption algorithms, and for strong authentication methods, such as Kerberos, RADIUS, and SSL.
- orapki Utility for Public Key Infrastructure Credentials Management
  The `orapki` utility manages certificate revocation lists (CRLs), creates and manages Oracle wallets, and creates signed certificates.
- Duties of Strong Authentication Administrators
  Most of the tasks of a security administrator involve ensuring that the connections to and from Oracle databases are secure.

23.1 About the Configuration and Administration Tools

The configuration and administration tools manage the encryption, integrity (checksumming), and strong authentication methods for Oracle Net Services.

Strong authentication method configuration can include third-party software, as is the case for Kerberos or RADIUS, or it may entail configuring and managing a public key infrastructure for using digital certificates with Transport Layer Security (TLS).

23.2 Native Network Encryption and Strong Authentication Configuration Tools

Oracle Net Services can encrypt data using standard encryption algorithms, and for strong authentication methods, such as Kerberos, RADIUS, and SSL.

- About Oracle Net Manager
  Oracle Net Manager configures Oracle Net Services for an Oracle home on a local client or server host.
- Kerberos Adapter Command-Line Utilities
  The Kerberos adapter provides command-line utilities that obtain, cache, display, and remove Kerberos credentials.

23.2.1 About Oracle Net Manager

Oracle Net Manager configures Oracle Net Services for an Oracle home on a local client or server host.

Although you can use Oracle Net Manager, a graphical user interface tool, to configure Oracle Net Services, such as naming, listeners, and general network settings, it also enables you to configure the following features, which use the Oracle Net protocol:

- Strong authentication (Kerberos, RADIUS, and Transport Layer Security)
- Native network encryption (RC4, DES, 3DES, and AES)
- Checksumming for data integrity (MD5, SHA-1, SHA-2)

> **Note:**
>
> The DES, 3DES112, 3DES168, MD5, and RC4 algorithms are deprecated in this release. To transition your Oracle Database environment to use stronger algorithms, download and install the patch described in My Oracle Support note 2118136.2.

23.2.2 Kerberos Adapter Command-Line Utilities

The Kerberos adapter provides command-line utilities that obtain, cache, display, and remove Kerberos credentials.

The following table briefly describes these utilities.

Table 23-1 Kerberos Adapter Command-Line Utilities

Utility Name	Description
`okinit`	Obtains Kerberos tickets from the Key Distribution Center (KDC) and caches them in the user's credential cache
`oklist`	Displays a list of Kerberos tickets in the specified credential cache
`okdstry`	Removes Kerberos credentials from the specified credential cache
`okcreate`	Automates the creation of keytabs from either the KDC or a service endpoint

> **Note:**
>
> The Cybersafe adapter is not supported beginning with this release. You should use Oracle's Kerberos adapter in its place. Kerberos authentication with the Cybersafe KDC (Trust Broker) continues to be supported when using the Kerberos adapter.

Related Topics

- Utilities for the Kerberos Authentication Adapter
  The Oracle Kerberos authentication adapter utilities are designed for an Oracle client with Oracle Kerberos authentication support installed.

23.3 orapki Utility for Public Key Infrastructure Credentials Management

The `orapki` utility manages certificate revocation lists (CRLs), creates and manages Oracle wallets, and creates signed certificates.

The basic syntax for this command-line utility is as follows:

```
orapki module command -option_1 argument ... -option_n argument
```

For example, the following command lists all certificate revocation lists (CRLs) in the CRL subtree in an instance of Oracle Internet Directory that is installed on `machine1.us.example.com` and that uses port 389:

```
orapki crl list -ldap machine1.us.example.com:389
```

> **Note:**
>
> The use of `orapki` to configure Transparent Data Encryption has been deprecated. Instead, use the `ADMINISTER KEY MANAGEMENT` SQL statement.

Related Topics

- Certificate Revocation List Management
  Certificate revocation list management entails ensuring that the CRLs are the correct format before you enable certificate revocation checking.
- Managing Oracle Database Wallets and Certificates
  You can use the `orapki` command line utility and sqlnet.ora parameters to manage public key infrastructure (PKI) elements.

23.4 Duties of Strong Authentication Administrators

Most of the tasks of a security administrator involve ensuring that the connections to and from Oracle databases are secure.

The following table describes the primary tasks of security administrators who are responsible for strong authentication, the tools used to perform the tasks, and links to where the tasks are documented.

Table 23-2 Common Security Administrator/DBA Configuration and Administrative Tasks

Task	Tools Used	See Also
Configure encrypted Oracle Net connections between database servers and clients	`sql.net` parameters or Oracle Net Manager	Configuring Encryption on the Client and the Server
Configure checksumming on Oracle Net connections between database servers and clients	`sql.net` parameters or Oracle Net Manager	Configuring Integrity on the Client and the Server
Configure database clients to accept RADIUS authentication	`sql.net` parameters or Oracle Net Manager	Step 1A: Configure RADIUS on the Oracle Client

Table 23-2 (Cont.) Common Security Administrator/DBA Configuration and Administrative Tasks

Task	Tools Used	See Also
Configure a database to accept RADIUS authentication	`sql.net` parameters or Oracle Net Manager	Step 1B: Configure RADIUS on the Oracle Database Server
Create a RADIUS user and grant them access to a database session	SQL*Plus	Step 2: Create a User and Grant Access
Configure Kerberos authentication on a database client and server	`sql.net` parameters or Oracle Net Manager	Step 6: Configure Kerberos Authentication
Create a Kerberos database user	• `kadmin.local` • Oracle Net Manager	• Step 7: Create a Kerberos User • Step 8: Create an Externally Authenticated Oracle User
Manage Kerberos credentials in the credential cache	• `okinit` • `oklist` • `okdstry` • `okcreate`	• okinit Utility Options for Obtaining the Initial Ticket • oklist Utility Options for Displaying Credentials • okdstry Utility Options for Removing Credentials from the Cache File
Create a wallet for a database client or server	`orapki` utility	Creating a New Oracle Wallet in the *Oracle Database Enterprise User Security Administrator's Guide*
Request a user certificate from a certificate authority (CA) for SSL authentication	`orapki` utility	• Adding a Certificate Request in the *Oracle Database Enterprise User Security Administrator's Guide* to add a certificate request • 6.5.2.3 Importing the User Certificate into an Oracle Wallet in the *Oracle Database Enterprise User Security Administrator's Guide* to import a user certificate into an Oracle wallet
Import a user certificate and its associated trusted certificate (CA certificate) into a wallet	`orapki` utility	• Importing a Trusted Certificate in the *Oracle Database Enterprise User Security Administrator's Guide* to import a trusted certificate • Importing the User Certificate into an Oracle Wallet in the *Oracle Database Enterprise User Security Administrator's Guide* to import a user certificate into an Oracle wallet
Configuring SSL connections for a database client	`orapki` utility	Configuring TLS Connection With a Client Wallet
Configuring SSL connections for a database server	`orapki` utility	Configuring TLS Using a Public Certificate Authority Root of Trust for the Database Server Certificate
Enabling certificate validation with a certificate revocation list (CRL)	`sql.net` parameters or Oracle Net Manager	Configuring Certificate Validation with Certificate Revocation Lists