IBM Security Verify Privilege

Distributed Engine Security Guide

Contents

Components of Distributed Engine

Secret Server Distributed Engine has three installed components: the Privilege Vault web server, the Site Connector, and the Engine. The web server generates messages and places them in the Site Connector. The Engine connects to the Site Connector and retrieves messages, processes them, and then hands the results back to Privilege Vault.

Privilege Vault organizes network locations through sites. A site is a virtual container for Secrets and Discovery Sources that belong within a specific network location. Each Secret and Discovery Source has an assigned site. Each Engine must be assigned to one & only one site.

Engine Authentication to Privilege Vault

When an Engine starts, it authenticates as follows:

Engine<->Privilege Vault Handshake

1) Engine calls Privilege Vault – Privilege Vault generates a public/private 4096 bit RSA key pair (Server Public Key and Server Private Key) and returns the Public Key (Server Public Key).
2) Engine creates an authentication request, which contains the identifying information for the Engine.
3) Engine generates its own public/private 4096 bit RSA key pair (Engine Public Key and Engine Private Key).
4) Engine encrypts its authentication request with the Server Public Key.
5) Engine submits the encrypted authentication request to Privilege Vault along with the Engine Public Key.
6) Privilege Vault decrypts the authentication request using the Server Private Key.
7) Privilege Vault processes the authentication request – creates an Engine record if necessary, checks activated status, etc.
    a. If the Engine is inactive or there is another authentication problem, an error message is returned.
    b. If there is no authentication problem, Privilege Vault pulls the appropriate per-Engine AES 256 symmetric key (Engine Symmetric Key) from the database, encrypts it with the Engine Public Key, and sends it back to Engine.
8) When Engine receives the symmetric key message, it decrypts it using the Engine Private Key and retrieves the Engine Symmetric Key. From now on, all communication between the Engine and Privilege Vault will use the Engine Symmetric Key.

Configuration Request

1) Engine sends message to Privilege Vault asking for its configuration information.
2) Privilege Vault responds with the Site, Site Connector connection information, Site Connector credentials, and the Site Symmetric Key (an AES 256 symmetric key used to encrypt/decrypt the messages for the Site) for the Engine.

Connecting to the Site Connector & Message Processing

1) Using the Site Connector connection information, Engine connects to the Site Connector and starts listening for messages for its Site.
2) When the Engine has capacity to process messages and messages are available, the Engine retrieves the message, decrypts it using the Site Symmetric Key, processes the message, and sends the result back to Privilege Vault.

Encryption & Sites

Each site has its own AES 256 Symmetric Key (Site Symmetric Key) that is used to encrypt & decrypt messages for that particular site. As a result, each Engine has access to at most one Site Symmetric Key. An example flow for a Secret Heartbeat is below.

1) Privilege Vault loads the encrypted Secret from the database.
2) Privilege Vault decrypts the Secret using the Secret's AES 256-bit key.
3) Privilege Vault creates a Secret Heartbeat message for the decrypted Secret.
4) Privilege Vault encrypts the message with the Site Symmetric Key.
5) Privilege Vault sends the message to the Site Connector.
6) An Engine assigned to the specific site connects to the Site Connector and retrieves the message.
7) The Engine decrypts the Secret Heartbeat message using the Site Symmetric Key.
8) The Engine processes the Secret Heartbeat message and creates a response object.
9) The response object is encrypted using the Engine Symmetric Key and submitted to Privilege Vault.

Site Symmetric Key Locations

The following diagram illustrates a scenario where Privilege Vault is configured with two sites (Site1 and Site2), with one Engine each (Engine1 and Engine2). Note that each Engine has access only to the keys it needs – namely, its own Engine Symmetric Key (for communicating with Privilege Vault), and the Site Symmetric Key for the Site it is assigned to. Engine1 does not have access to the Engine Symmetric Key for Engine2, nor does it have access to the Site Symmetric Key for Site2. As shown below, the Site Connector does not have access to any of the keys, and thus cannot decrypt any of the messages it holds.