Disaster Recovery, Security, and High Availability

This document outlines the Disaster Recovery (DR) steps for Privileged Identity and how the solution can be made highly available.

Disaster Recovery Preparation

As in any application a good backup strategy for your system and its system state information is imperative and should be implemented for all components. While this holds true for Privileged Identity, it is important to understand that some components of Privileged Identity are much more important than others.

Privileged Identity is divided into three components:

- Management Application (or Console), including Deferred Processor & Encryption Key
- Database
- Web Site

The database is the single most important component to Privileged Identity. All systems lists, jobs, job settings, passwords, and other information about the systems are stored here in the database.

If you have implemented a backup solution for your system which includes all system state information and the web site, database, and management application, and they are all installed on the same system, this will be sufficient for recovery. If the database, management application, and web site are on separate systems then you will need to be aware how the individual components of Privileged Identity work.

The Privileged Identity database must be part of the normal backup regiment. As Privileged Identity uses Microsoft SQL or Oracle for the database, you will use programs and APIs for database backup that are native to Microsoft or Oracle; BeyondTrust does not provide a backup mechanism to manage Microsoft SQL or Oracle database backups.

Generally, backup the program database at least as often as scheduled password change jobs run. It is recommended to perform nightly full/complete/normal backups of the production database. The database is comparably small - typically no more than a couple hundred megabytes, but can be gigabytes depending on the scenario.

It is highly recommended to turn on encryption for the stored passwords in the database. If password encryption for the password information in the database is enabled, it will be necessary to archive the encryption key that Privileged Identity uses. The encryption settings are located under **Settings | Encryption Settings** within the management application. From the **Encryption Settings** dialog, choose to export the encryption key. This encryption key only needs to be exported as often as the encryption key is changed.

Disaster Recovery

Once the database is restored, Privileged Identity can be reattached to the database. If reinstalling Privileged Identity, the installer will prompt for the Privileged Identity database - simply choose the same database. If you had enabled encryption previously, you will need to re-import the encryption key. This can be done from **Settings | Encryption Settings** within the management application.

The web site functions independently of the management application. This means a failure of the management application will not render the passwords inaccessible. If the web site should become unavailable for any reason and restoration is not possible, simply re-deploy the web site from the management application. Refer to thePrivileged Identity installation guide for specific steps. All settings will remain intact and all delegations will still remain intact.

Ultimately, the backup of the program database and encryption key is all that is required for Privileged Identity to be restored to any system. Without both of these items, it will not be possible to gain access to the random passwords stored in the database.

Licensing is stored in the database rather than locally. When multiple consoles are present, and at least one console experiences total host system disaster, it may be preferred to properly license any one of the other hosts or install a new console.

If the original host is lost and a new host must be brought online to support management console functionality, a new license will be required for the new host if the name has changed. If a key has already been supplied to you, go to **Help | Register** to input the key. If a key has not been supplied to you then contact your account manager for a replacement key (replacement meaning the original licensed console will not be restored to a functional state). The original encryption key will be required for this installation to maintain access to the original database for password retrieval and management purposes.

Privileged Identity is agnostic of the database or database server it connects to. This means you are free to move the database to any system at any time, though if the name of the database server changes, the management application and web sites will need to be redirected to the new database. This can be done by changing the database options from **Settings | Database Configuration** for the management console, and then updating the web site connection settings by going to **Settings | Manage Web Application | Manage Web Application Instances** and choosing to update the instance with current options.

High Availability

As in any application a good backup strategy for your system and its system state information is imperative and should be implemented for all components. High availability is more than just a good backup strategy; it is ensuring that the services which provide the data are available to you with the least downtime and as little interruption to service as possible. This means that items like mirroring and clustering need to be addressed.

The Database

The database is the single most important component to Privileged Identity. All systems lists, jobs, job settings, passwords, and other information about the systems are stored here in the database.

For Microsoft SQL Server, high availability options include Database Mirroring and Clustering. For Oracle, use Mirroring (Active Data Guard) or clustering (RAC). Mirroring is cheaper than clustering but requires more work in a Disaster Recovery scenario. For steps on how to configure mirroring or clustering, see the Microsoft or Oracle documentation associated with your database.

Where mirroring is concerned, if the database fails, a secondary server with the same information is readily available. In this scenario, redirect Privileged Identity and its web site(s) to the mirrored database. To do this, go to **Settings | Datastore Configuration** and input the new database server name. Some companies further this process by having a monitor examine the health of the database servers. If the master mirror fails, the DNS records are automatically redirected to the secondary mirror. This process ensures no program reconfiguration is required.

In regards to clustering, if the active node of the database fails, the secondary server will take over automatically and there will be no discernible interruption to service nor a need to reconfigure Privileged Identity or the web site(s) in any way shape or form.

The web site

The web site works independently of the management application. This means that even if the management application crashes, the web site will still be able to function and serve requested passwords. To avoid loss of this functionality, BeyondTrust recommends the use of Network Load Balancing (NLB) for the web site. NLB will require each of your web servers to have two IP addresses - one for each system and a common one for the NLB cluster. For specifics about setting NLB for your version of Windows, please see your Microsoft documentation.

When using NLB, the web site is referenced through a single name (just like clustered databases) and if one is busy or offline, the other(s) will take over. Be sure to turn off session state management within the IIS web site/virtual directory settings.

The Management Application

For the management application, there is presently no built-in clustering solution available. Rather, if an enterprise license or DR application was purchased, you can install the application multiple times on multiple systems and direct them to the same database. If you do not choose to obtain an enterprise license or DR application and are only able to install one licensed application, in the event of disaster of the system hosting the application, there will still be no interruption to password recovery or availability. This is because all of the data is stored in the database and password recovery is supplied through the web site. In the absence of the management application, management of systems lists and job creation will be unavailable until the application is reinstalled and attached back to the original database. Once the management application is reinstalled and reconnected to the original database, all groups, systems, and jobs will be completely intact.

The installation process for the management application is comprised of accepting the End-User License Agreement and choosing the installation directory. This will take very little time - as long as it takes you to click **Next**, **Next**, **Next**, **Next**, **Finish**.

Total Failure

The question will come up: *If I didn't backup or all my backups failed, and the database completely failed and I didn't do clustering, mirroring, log shipping, or similar, then what happens to my stored passwords?* The answer is: *It depends on the target system.*

For trusted systems, simply begin randomizing passwords again using your domain authority. For untrusted systems (standalone devices, etc), it may require a reset of the password or authoritative restore of a base password using various products.

Like any important system, it is always recommended to test the backups and examine and monitor system health.Privileged Identity integrates with various SIEM systems such as Microsoft System Center Operation Manager and ArcSight Enterprise Security Manager for such monitoring and alerting.

Security

As previously mentioned, the database is the single most important component to Privileged Identity. All systems lists, jobs, job settings, passwords, and other information about the systems are stored in the database. This means your foremost goal will be to secure the database and how it can be managed or connected to.

First, if using Microsoft SQL Server, implement the use of integrated security for the database. This will enable you to limit who has access to the database even if they have access to the management application as each user must then be authenticated to the database. If using SQL authentication, then it will always appear as the SQL account is the one which accesses the database and accountability will be greatly minimized.

Next is to control who has access to the management application. By default, anyone who is an administrator on the system where the management application is installed will have the ability to launch the tool (though security on the database will prevent access to the data). This, however, may not be the desired behavior. To control which administrators have the ability to even launch the management application, go to **Settings | Delegations | Delegate Console Access** and define which user(s) will have the rights to launch the console.

If two-factor authentication is configured for the user and the machine, Privileged Identity can also require the user(s) to use their two-factor authentication to gain access to the management application and/or password recovery web site.

Change the default password recovery access password from within the management application and configure event sinks to alert on the attempted access to the dialog. The steps for each of these items are outlined in the Privileged Identity admin guide.

Although the web site does not retrieve a clear text password from the database when encryption is enabled, the web site does not include its own protection mechanisms when passing passwords to the user's browser and is reliant on the methods implemented within IIS. This means configuration of SSL encryption within the IIS server is of paramount importance. Further, IIS supports the use of user-based certificates and these can be used to authenticate users as well.

Privileged Identity supports web sites which employ the use of two-factor authentication. This requires the user to be configured for two-factor authentication and the user to be required to use them within the web site, which is one of the delegation options. View the documentation on the product web site for exact steps on how to configure two-factor authentication.

When passwords are recovered in the web site, one of the configuration options when setting up the web site is to send an administrative alert to this effect. This will alert the specified parties that these passwords are being recovered. This is not turned on by default but is highly recommended. View the documentation on the product web site for exact steps on how to configure these alerts.