WHITEPAPER

How to Access Privileged Passwords in ‘Break Glass’ Scenarios

BeyondTrust

Contents

Introduction 3
Break Glass Use Cases 3
The Break Glass Process 4
Break Glass for Environments Using a Password Manager 4
Break Glass and Session Management 6
When a Password Management Solution Contains Stale Passwords 6
Application-to-Application Passwords and Automated Workflows 7
Physical Paper Password Storage 8
Restoring Order After a Break Glass Incident 8
How BeyondTrust Password Safe Enables Break Glass 9
More about BeyondTrust Password Safe 11
The BeyondTrust Privileged Access Management Platform 12
About BeyondTrust 13

Introduction

Break glass is a term used in computing to describe the act of checking out a system account password for use by a human user when an emergency arises and traditional access methods have failed. The term derives from the act of breaking the glass on a fire alarm.

Access controls in an application or asset can be bypassed during a critical emergency by using break glass. A user performs a break-glass check out or release of the account and password (credentials) when he or she needs immediate access, even if the user is not authorized to manage the system. This method is customarily used for the highest-level system accounts, such as root accounts for Unix and Linux, SYS or SA for a database, or administrator for Windows (local or domain). These highly privileged accounts are not usually assigned to a specific person, so instead, break glass limits their utilization with various controls to reduce risk and enable only specific tasks. It is obvious, however, that user access to break glass credentials is still restricted and not as accessible as a fire alarm.

This technical brief will discuss break glass scenarios that involve operational anomalies within your environment—such as those caused by a network outage, application fault, or natural disaster—that disrupts the normal availability of your privileged password management solution. Therefore, factors like power source and network connectivity should be considered when designing your break glass policy.

Break Glass Use Cases

Break glass scenarios are usually considered when information technology administrators are deploying critical infrastructure to secure system access. Here are three common break glass scenarios applicable to most organizations:

1. Requirement for emergency, direct access to managed systems using a password as an enabler.
2. Getting access outside of the standard operating process because mission critical systems are down, or a required approver is unavailable.
3. Retrieving passwords or secrets from a physical safe or other offline backup on a physical device such as USB drive/CD.

The Break Glass Process

When developing a break glass policy, there are a few important considerations and potential processes to implement:

1. For authorized break glass users (new or existing), consider creating pre-staged emergency user accounts that are managed and distributed in a way that can make them quickly available without administrative delay but have the appropriate restrictions to protect from a threat actor. The break glass accounts and distribution procedures should be documented and tested as part of implementation, and carefully managed to provide timely access when needed. These can be stored in the password manager or a physical secure location, and have paper counterparts stored in another media, or highly secure environment.

2. To comply with auditing requirements, even if an approval is bypassed, the system should still fully log who has access and what actions were performed. Additionally, IT administrators should review the logs to ensure compliance with change management processes when a break glass process is used.

3. Break glass processes that are implemented outside of the password management technology, such as a physical safe and storage of printed passwords, should be routinely updated and manually tested for effectiveness and change control. Only select users should have access to the combination or keys to the physical safe and they should be treated like any other sensitive information within the organization.

Break Glass for Environments Using a Password Manager

Information technology (IT) organizations often utilize a password manager as a break glass solution to provide access into their environment when the established processes for login or authentication fail. IT teams might authenticate with LDAP, AD, or multifactor, and the user would log in prior to using sudo or a least-privilege solution to gain limited administrative privileges. When this method fails, the break glass process would require IT to provide a password for an account within established parameters (timeframe, privileges, scope, etc.) to access the application or system.

During normal operation, users who need access to privileged passwords will access the tool to retrieve a password or establish a session so that they can perform whatever tasks or operations are assigned for their roles. This requires that the password management solution have the rights to fully manage, rotate, and keep the password current. Relying on end-users to diligently remember, rotate, and securely document all their passwords is invariably less reliable and poses a heightened risk.

When using a password manager, consider these break glass use cases:

1. The person who needs a managed password cannot log in to the solution

a. Repair user access to the password manager
b. Reset the managed credentials
c. Reset the password for the user accessing the solution

2. Fault authenticating to the password management solution

a. Repair network connectivity for critical paths
b. Restore password management connectivity to critical authentication services
c. Repair authentication system
d. Store a printout of the passwords in a highly secure location

3. The password management solution is not available

a. Repair network connectivity
b. Access solution through fault-tolerant node

4. Managed passwords are invalid

a. Refresh the password by using the solution to automatically generate a new one
b. Use the password history feature of the password manager to determine the last valid password

5. Connectivity anomaly

a. When critical services are not functioning, access may be required via iDrac, management networks, or crash carts
b. When network connectivity does not allow access, lateral connectivity not subject to segmentation, can provide break glass access

6. Processes and workflow prevent access

a. No approver is available in the time period required
b. User access is restricted due to system ownership, such as employee role, contractor, or vendor
c. Time of day constraints or critical event requires immediate unrestricted access

Break Glass and Session Management

For this use case, the enterprise password management solution enforces connectivity through the session manager to document activity, security controls, and command line filtering, by managing connections through the network, and enforcing segmentation. By design, there is no alternate way to connect to the network without first accessing the session manager. One option for achieving break glass access would be to drop security controls in order to restore availability.

However, as with all risk-based decisions, it is important to review and document the risks and benefits, and get organizational alignment. Moreover, management networks controlling remote access or terminal servers may provide a safer, alternate approach as opposed to reducing security controls in a break glass scenario—especially if the event that caused the disruption is security-related. Therefore, access to session managers during break glass scenarios should include the following:

1. Controlling third-party access to managed systems
    a. Open alternate access into the environment via backup connections
    b. Repair session management access to the primary systems
    c. Access session management in an alternate datacenter

2. Controlling internal access to managed systems
    a. Repair session management access
    b. Open network path around the session management device
    c. Access session management device in an alternate datacenter

When a Password Management Solution Contains Stale Passwords

There are many situations where a password stored in the password manager may be stale through no fault of the technology. Such cases could arise due to restoration of backup images, roll back of virtual snapshots, or even the deployment of a new instance or system based on a template. In these use cases, the break glass password manager has automated the rotation of passwords of human, service, or built-in accounts throughout the environment. Consequently, no one knows the correct password, and the password is not written down for manual retrieval. During normal operation, password managers will randomize and change the passwords, update managed systems, and store and test the new password.

So, what do you do when this process fails? Here are some recommendations:

1. If the tool cannot change a single or small number of passwords:
    a. Repair connectivity or retool the configuration of the system to make password changes based on the uniqueness of the targets

b. Manually change password, using another account (typically called the "Functional Account") that has privilege

2. If the tool cannot change any passwords:

a. Repair network connectivity
b. Verify Functional Accounts have proper privileges to manage passwords remotely

3. If the password of a built-in account is not known:

a. Randomize the password of the built-in account using the Functional Account
b. Repair system by booting to a single user mode and change password

4. If the password of a service account is not known, so a service will no longer start:

a. Randomize the password of the service using the Functional Account
b. Establish a privileged connection to system using a stored credential and manually set the service account password before automating password management.

Application-to-Application Passwords and Automated Workflows

In these use cases, IT administrators or developers have implemented a password manager to forgo hardcoded passwords in configuration files, scripts, or compiled applications. Instead, the application, script, or configuration file accesses the password manager via an Application Programming Interface (API) to retrieve the current password it needs to complete the processing operation. The application can potentially cache the password for continuous use, or release the password when it is complete. To do so, the environment must allow for password changes while applications are running. IT administrators must know the process for rotating and refreshing passwords mid-cycle.

Here are some recommended steps:

1. If automation jobs develop a fault:

a. Repair the password management solution
b. Enable fault tolerance for the API
c. Add caching to the scripts, configuration, or application to be fault tolerant for a network, connectivity, or password management outage
d. Manually update jobs and resubmit; ensure that all dependencies have been met.

2. If automation jobs require change control for password changes:

a. Schedule password changes during maintenance windows

b. Develop applications that are fault tolerant or can be resumed in the event of an API query failure for any reason

Physical Paper Password Storage

Your recovery plans should also include the ultimate break glass solution—retrieving physical copies of passwords. There are inherent risks with storing physical copies of privileged passwords. However, with the proper physical controls in place to securely store the credentials, physical storage of paper can serve as an option in break glass scenarios.

Recommendations for this use case include:

- Create a plain text copy of the credentials and automatically print them in a secure location or store them on reliable removable media. Regardless of the format, paper or offline digital removable media, ensure that final storage is highly secure.
- If your processes require, re-encrypt the digital media with an offline encryption package prior to writing to a USB drive or CD. Remember to back up the password for the offline encryption in a secure location as well.
- Fully document the process for creating and storing break glass passwords. Passwords should be rotated and restored on a regular basis.
- As with any disaster recovery process, the paper or removable media process must be tested periodically to ensure its reliability.

Restoring Order After a Break Glass Incident

After a break glass event, the recovery process to normal operations should entail considering a few security and operational events. While these may seem esoteric, the purpose of break glass process is to provide access in a worst-case scenario. If restoration is provided too quick, or change control and checks and balances are not verified, the break glass process could be used against the organization in a future attack, or just lead to another similar disruptive event in the future.

Therefore, consider the following before restoring normal services:

- What event occurred requiring the break glass process?
- Can this event be avoided in the future?
- Was the access to break glass credentials appropriate?
- Were there any resources in the break glass process that did not have coverage?
- Who was notified of execution of the break glass process?
- Was any additional risk (data loss, resource exposure, etc.) introduced by the process?

If these questions can be answered satisfactorily, and no critical action items arise in response, services can be resolved to normal operations. Once operations resume, continue with the following queries:

- Was the restoration process of services accurate after a break glass event? If not, how can it be improved or fixed?
- Were all electronic credentials and passwords reset after the break glass event?
- Was all physical storage of credentials reinstated and codes to physical storage reset?
- Was all break glass session activity verified and audited for inappropriate activity?

If break glass scenarios repeatedly occur, then the entire process should be evaluated to prevent their invocation in the first place. This could be anything from faulty hardware, network anomalies, to the unavailability of key personnel in a critical need situation. The restoration to normal services should always include the complete post-mortem of the break glass key event.

How BeyondTrust Password Safe Enables Break Glass

Credentials that must be accessed outside the organization can be challenging to lock down. To get it right, you need to apply context to the access – all the runtime parameters of the request must be evaluated to enforce appropriate access.

Who is trying to log on?

What system are they trying to access?

Where are they logging in?

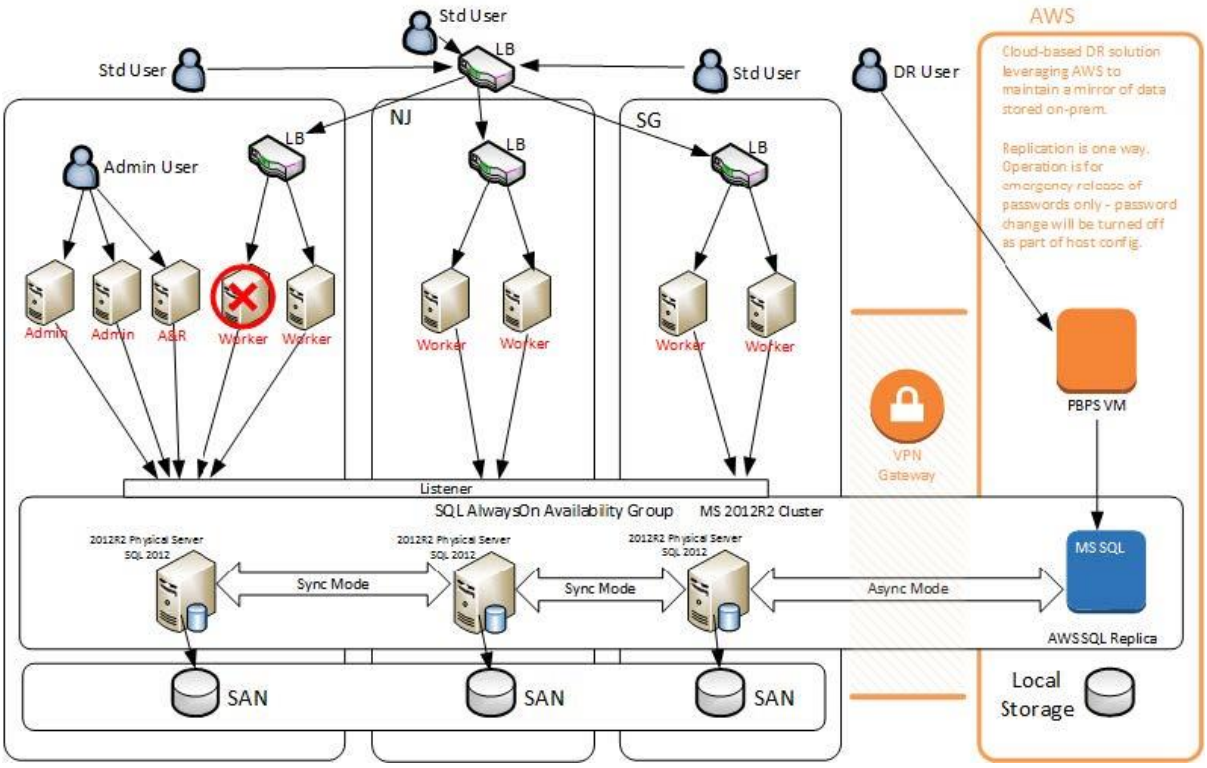
What day of the week is it?

What is the time of day?

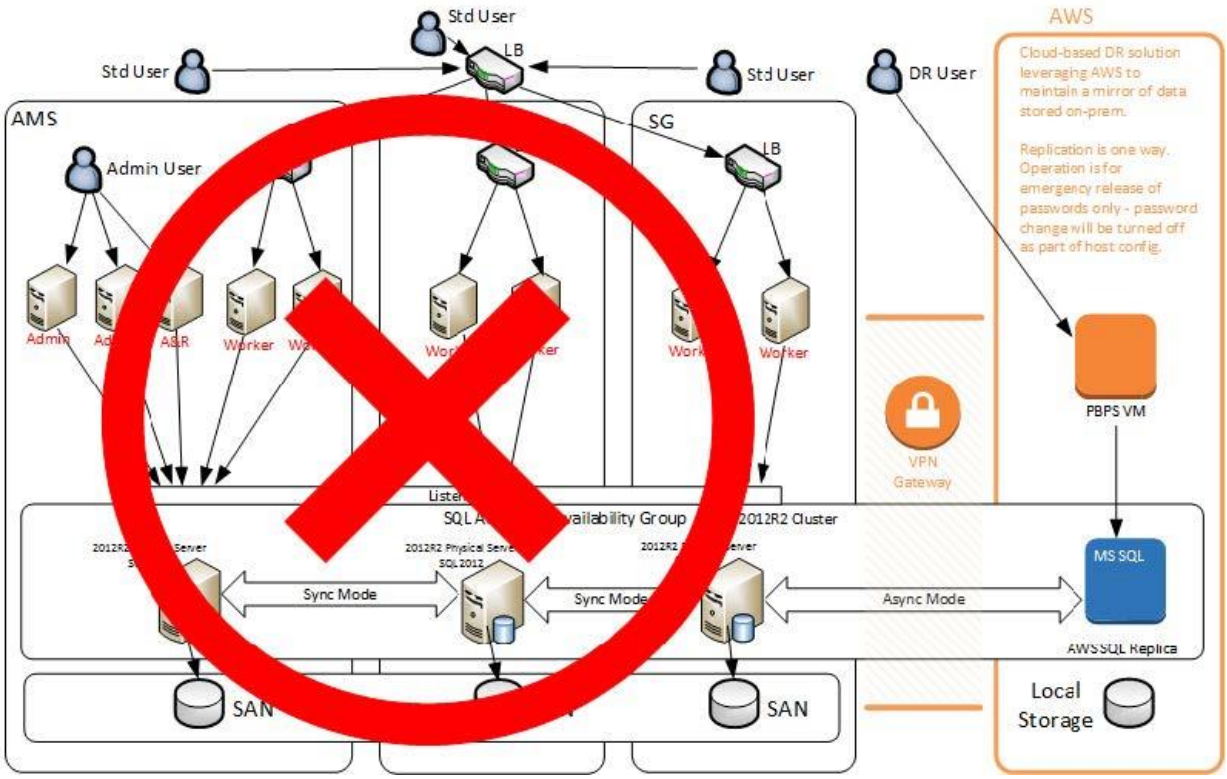
Applying context allows you to incorporate privileged access management best practices to better protect your organization from a breach. For example, if your break glass account is strictly for emergency use, only make it available during off hours. If it is expected that the account would be accessed via a remote employee working from home, verify that the request is coming in via the VPN concentrator.

BeyondTrust's Password Safe provides a secure connection gateway, with the ability to proxy access to RDP, SSH, and Windows applications. Leveraging dynamic assignment of just-in-time privileges via Advanced Workflow Control, organizations may lock down access to resources based upon the day, date, time, and location.

Break Glass – Password Safe



Password Safe has multiple levels of redundancy to mitigate the risk of data loss. Flexible high availability deployment architectures ensure that passwords remain available whether everything is installed in a single datacenter, or across multiple geographic locations. This is traditionally the first line of architecture and defense before utilizing a break glass process.



For short-term outages of the entire on-premise infrastructure, passwords may be retrieved via cloud environments, such as Amazon Web Services or Azure. This would need to be properly secure and architected as a part of the initial design. Finally, emergency access to Password Safe may require release of passwords manually stored in physical safes to layer on the proper protection.

More about BeyondTrust Password Safe

BeyondTrust Password Safe provides visibility and control over all privileged accounts and SSH keys, as well as over the assets and systems they protect. The BeyondTrust solution includes robust session monitoring and management capabilities, which ensure maximum security, fine-grained visibility, and full accountability.

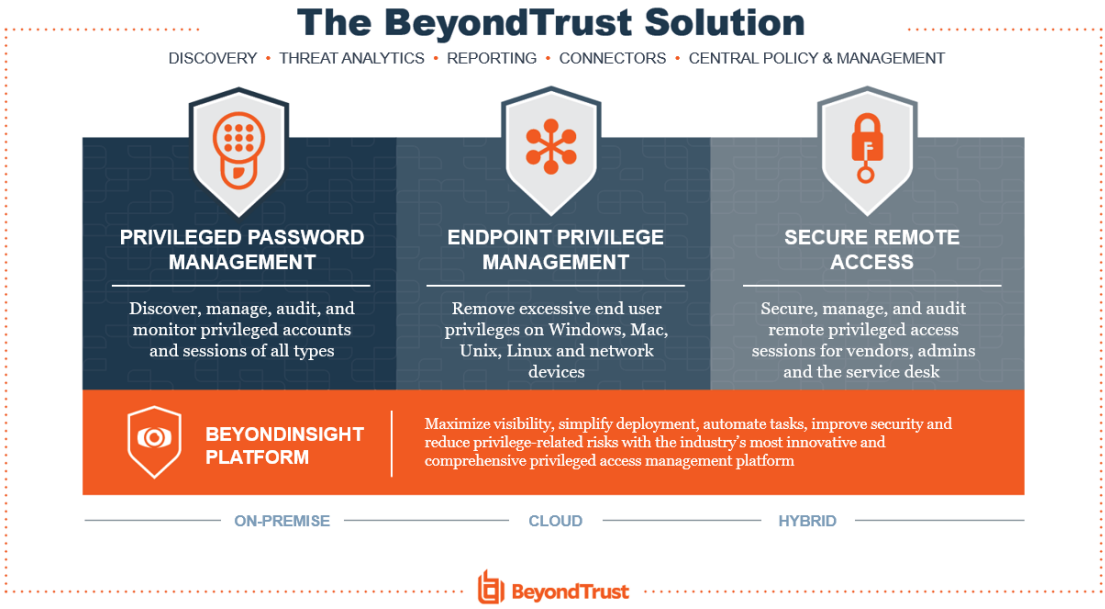
Password Safe offers secure access control, auditing, alerting, and recording for any privileged account – from local or domain shared administrator, to a user's personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts – even to SSH keys, cloud, and social media accounts.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.