WHITEPAPER

PASSWORD SAFE DEPLOYMENT AND FAILOVER GUIDE

BeyondTrust

TABLE OF CONTENTS

Introduction & Supported Deployment Methodologies

BeyondTrust Password Safe is an automated password and session management solution that provides secure access control, auditing, alerting and recording for any privileged account – such as a local or domain shared administrator account; a user's personal admin account; service, operating system, network device, database (A2DB) and application (A2A) accounts; and even SSH keys, cloud and social media. By improving the accountability and control over privileged passwords, IT organizations can reduce security risks and achieve compliance objectives.

This document describes 3 common deployment methods and examines scenarios that demonstrate disaster mitigation following loss of access to either primary components, or entire sites within a given environment. The quantity and location of components are in this document for illustrative purposes only.

Disaster Recovery (DR) use cases to consider when reviewing this document:

- In a DR scenario, do people need to go to through the session proxy?
- Do you execute a password change action while in DR?
- In a DR scenario, do you need the user ID's to be the same as in primary?
- Does everyone have the same role in a DR Scenario?
- Do the groups match, systems match, and deployment scenarios match?

Many different configurations are supported to scale from single site installations to multi-site, geographically dispersed environments. This document will outline the following:

Active/Active

Sometimes called multi-active, this deployment type allows multiple nodes (Password Safe instances) to be active at one time. Each node is connected directly to the database.

Advantages

- Unlimited scalability
- Redundancy of components
- Targeted password change events for specific locations

Disadvantages

- Requires an external database
- Redundant database configurations such as SQL Always On are expensive
- It is the responsibility of the customer to ensure that the database is securely hardened

Active/Passive

Two appliances are required for active/passive. The internal databases are replicated, and a heartbeat sent from the primary indicates to the secondary if it should take over operations.

Advantages

- Easy to set up
- All HA is incorporated within the solution

Disadvantages

- An external load balancer is required for auto-switching users to the active appliance
- The failover process can take 10 minutes or longer

Single Appliance with VMotion

For deployments where only one appliance is desired, VMware vMotion can be used to keep the UVM virtual appliance continuously available even if the physical server running the virtual image goes offline for any reason.

Advantages

- Cost effective HA with a single appliance
- Provides HA and continuous operation during host server outages

Disadvantages

- Relies on VMware vMotion to be setup and configured correctly
- Does not provide redundancy in the event of a software failure

Active/Active Architecture

The Active/Active deployment model is available for any mix of hardware and virtual appliances as well as software installation. It requires the use of an external database – we recommend Microsoft SQL Server AlwaysOn for scalability, but Password Safe has also been tested against SQL Standard and Enterprise editions (2012, 2014, and 2016).

As many appliances as required can be configured to connect to the database. In this case, all appliances can be used at once, and are fully redundant; if one goes down, you simply switch to an alternative. AlwaysOn Availability Groups may be configured with a mix of synchronous commit and asynchronous commit replicas to provide real - time database redundancy.

Database Configuration

The deployment and configuration are the responsibility of the customer but the following guidelines should be noted in the creation and configuration of the replicas:

The database must be created by our Software during the installation process. It cannot be created beforehand. After the database has been created apply the settings below:

- SQL data and log files should be placed on separate volumes and isolated from other applications using the same volume if possible.
- Default collation

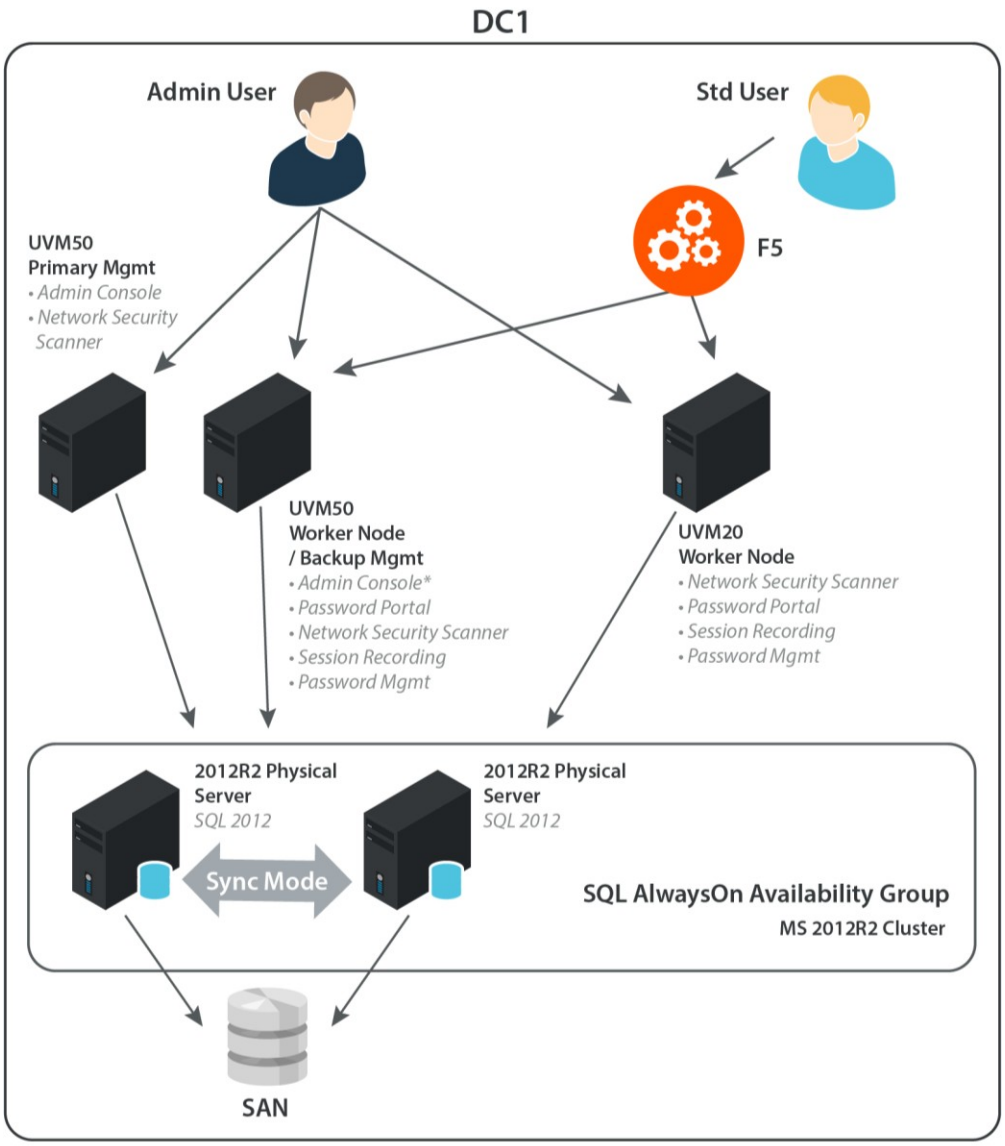
Data file size should be initialized at 300GB (will vary according to scoping)

- Log file size should be initialized at 30GB (will vary according to scoping)
- Auto growth should be on and set to a fixed amount (recommend 3GB) instead of a percentage (will vary according to scoping)
- Instant file initialization should be enabled
- Tempdb should be moved to a non system drive if possible
- Shrink should not be enabled, can be done manually in certain scenarios if necessary

A maintenance plan should be in place to regularly backup the transaction log, this should keep the file growing infinitely.

The number of nodes in the Availability Group will depend on customer requirements, as will the name of the nodes and listener. When creating the database during the installation process you will point to the address of the group listener. Once the database has been created you can make it available in AlwaysOn. Steps on adding to AlwaysOn can be found here: https://msdn.microsoft.com/en-us/library/hh213078(v=sql.120).aspx

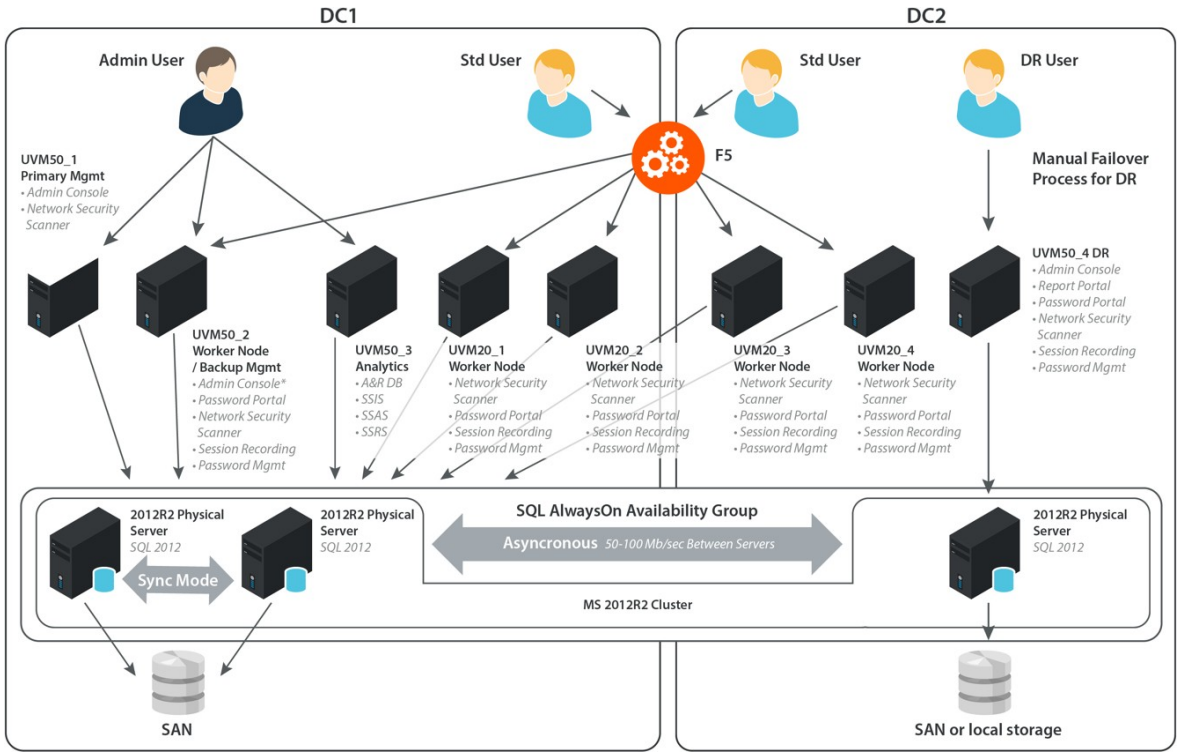
Single Site Deployment



A single site may contain a number of appliances for redundancy.

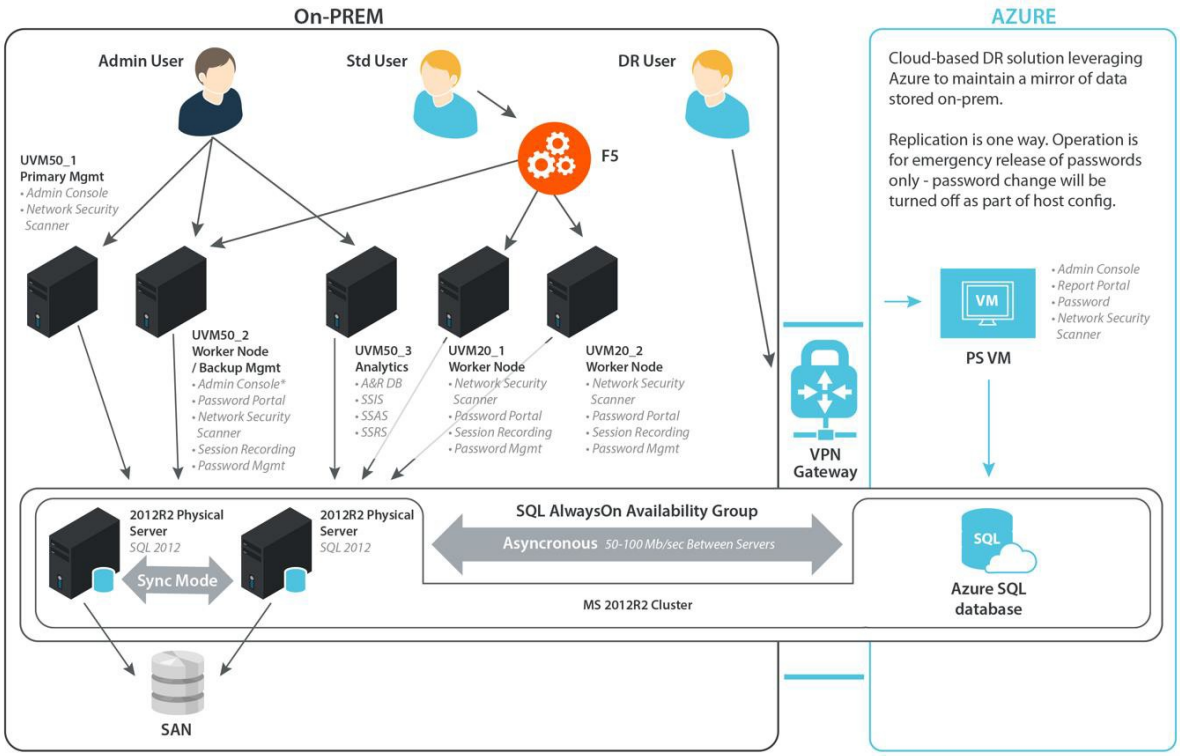
In this scenario, a pair of replicas are configured for synchronous commit within an external AlwaysOn Availability Group - this provides database redundancy. Three appliances are connected to the external address of the Availability Group. One is configured with a management console role, the other two are 'worker nodes'. Access to appliances may be made directly, or via load balancer. Both appliances may be used simultaneously; session recordings will be stored on the appliance in use – recordings may optionally be sent to a separate archive server based on disk utilization and/or retention.

Multi-Site Deployment



In this example, multiple datacenters are connected to an AlwaysOn Availability Group. It can be seen that many more appliances can be added, each with varying roles: Scanners; Event Servers; Password Portals, Session Managers; Password Management. Behind load balancers, appliances may be added for redundancy, and scalability; for example, session managers configured to send recordings to archive servers can be brought down with no loss of data or functionality. In this example, an additional async commit replica has been added to provide a DR capability. An additional appliance in the DR site is pointed to the DR replica for retrieval of passwords if access to the main infrastructure is lost. As many appliances may be added as required and pointed at the availability group. Note that only one manager service is supported but this may be configured to fail over to a secondary appliance. Also note that SQL has a single master model, therefore only one replica will have write access at any one time; however, replicas may be located in multiple locations for the event of database failover.

On-Premise with Cloud DR Deployment

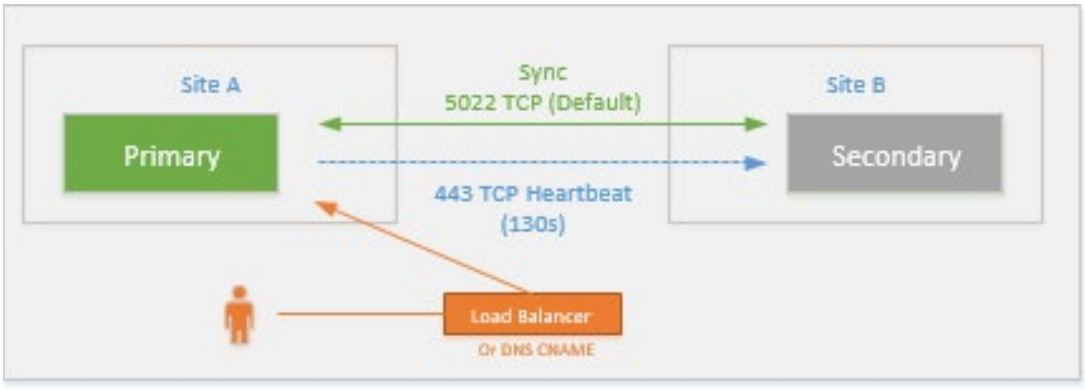


In this example, we are using Azure to store a replica of Password Safe so that in the event that all on premise components fail, operation may continue by releasing passwords from the Cloud. Microsoft SQL AlwaysOn Availability Groups may consist of a primary replica, and up to 4 secondary replicas in either synchronous - commit or asynchronous-commit. Replicas are supported in both Azure and AWS environments; a typical deployment model comprising an asynchronous replica in the Cloud provides access to password data in the event that all on-prem components become unavailable.

Active/Passive

Active/Passive is for appliances only. It will failover to a mirrored appliance in the event the primary appliance is not available. Failover is automatic. This method will involve 2 appliances configured as a 'pair'. Note that appliance pairs have to be identical i.e. UVMv20 -> UVMv20, UVM50 –> UVM50, UVM20 -> UVM20.

Non-Failover Stage

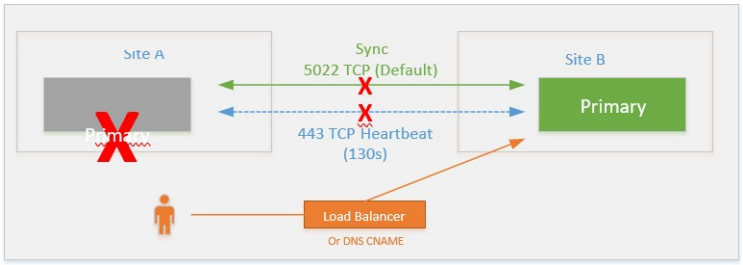


The database is mirrored via port 5022 (configurable).

A heartbeat is sent from the primary appliance to the secondary appliance every 130 seconds (non-configurable). If a heartbeat has not been detected for 14 minutes (default*), the secondary appliance will promote itself to a primary.

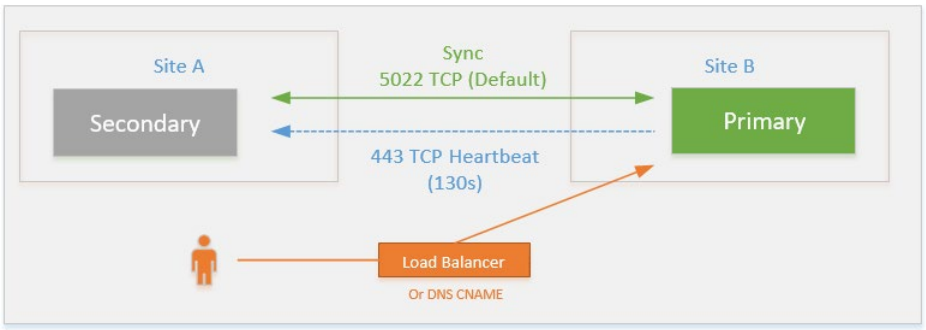
*range: 5 - 10,000 minutes

Failover Stage



Secondary appliance promotes itself to primary and starts servicing requests.

Recovery Stage



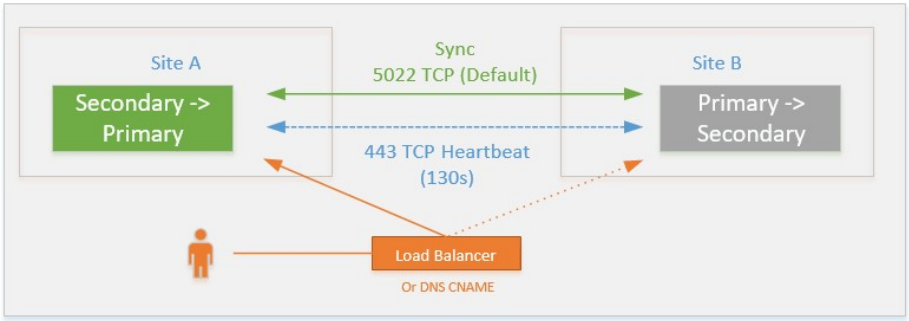
When the previous primary appliance in Site A starts up, it looks for a replica partner.

If the replica is found, the Site A appliance will start in secondary mode, and the database is replicated from Site B.

Please Note: As recovery takes place, the new primary in Site B will be taken offline as the database is replicated.

At this point, the appliances will remain with their current roles; Site B will continue to be primary, and Site A will become the new secondary.

Role Reversal

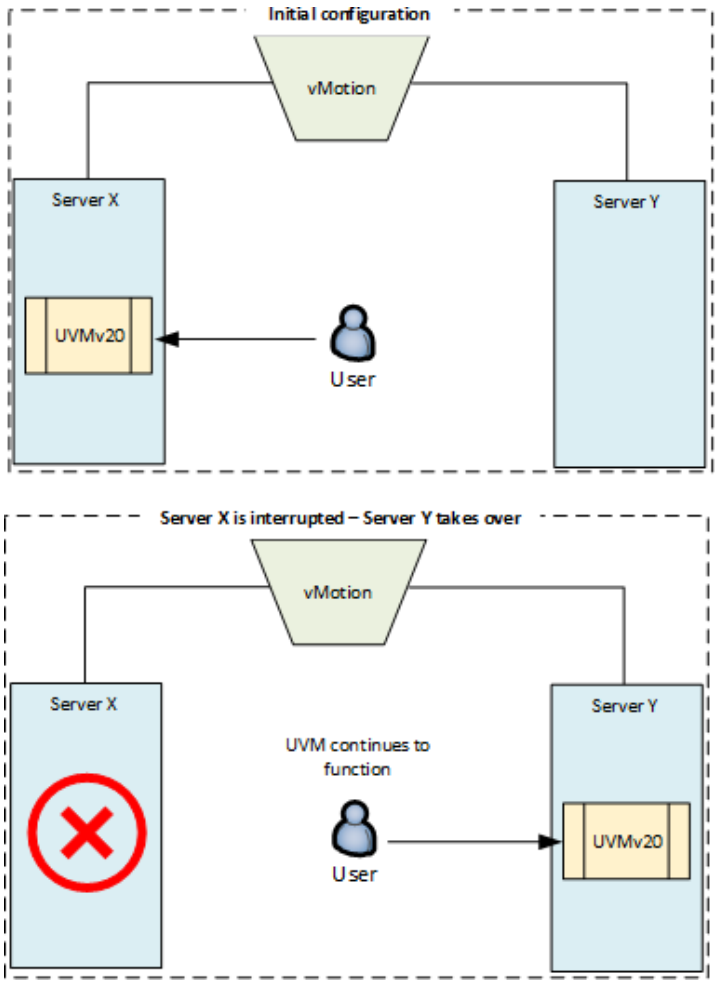


If it is desired that roles be reverted, wait for replication to complete then the following manual steps are performed:

Disable HA on Site B (breaks pair)

Enable HA on Site A (re-establish pair with new primary being Site A)

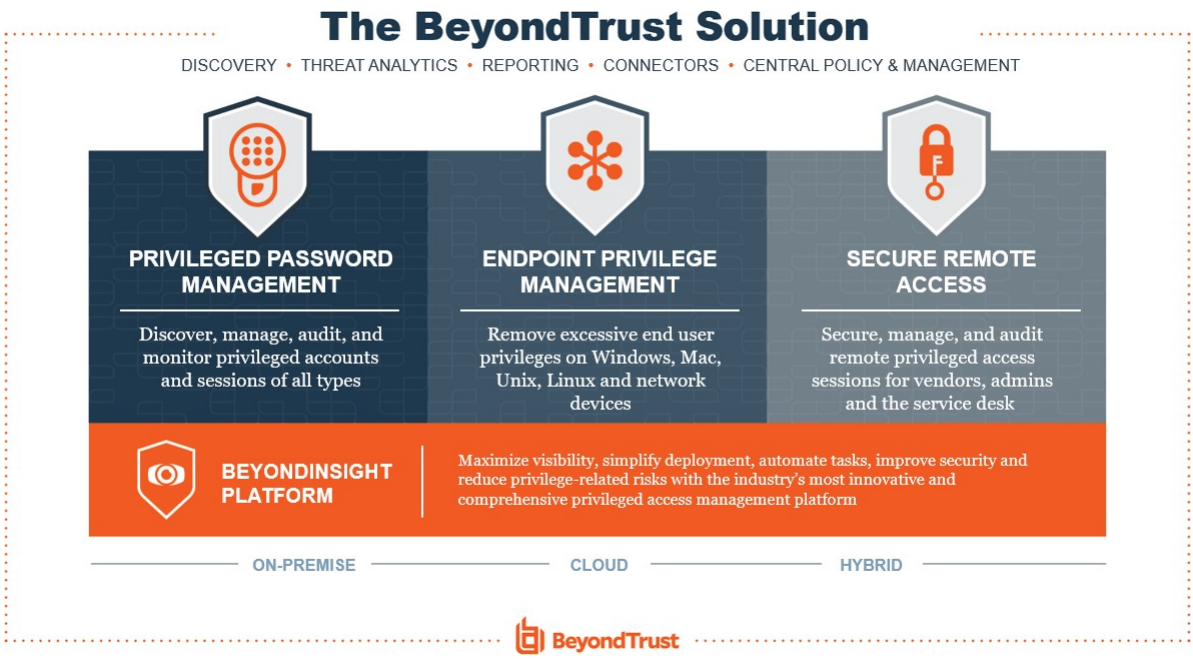
Appliance with vMotion



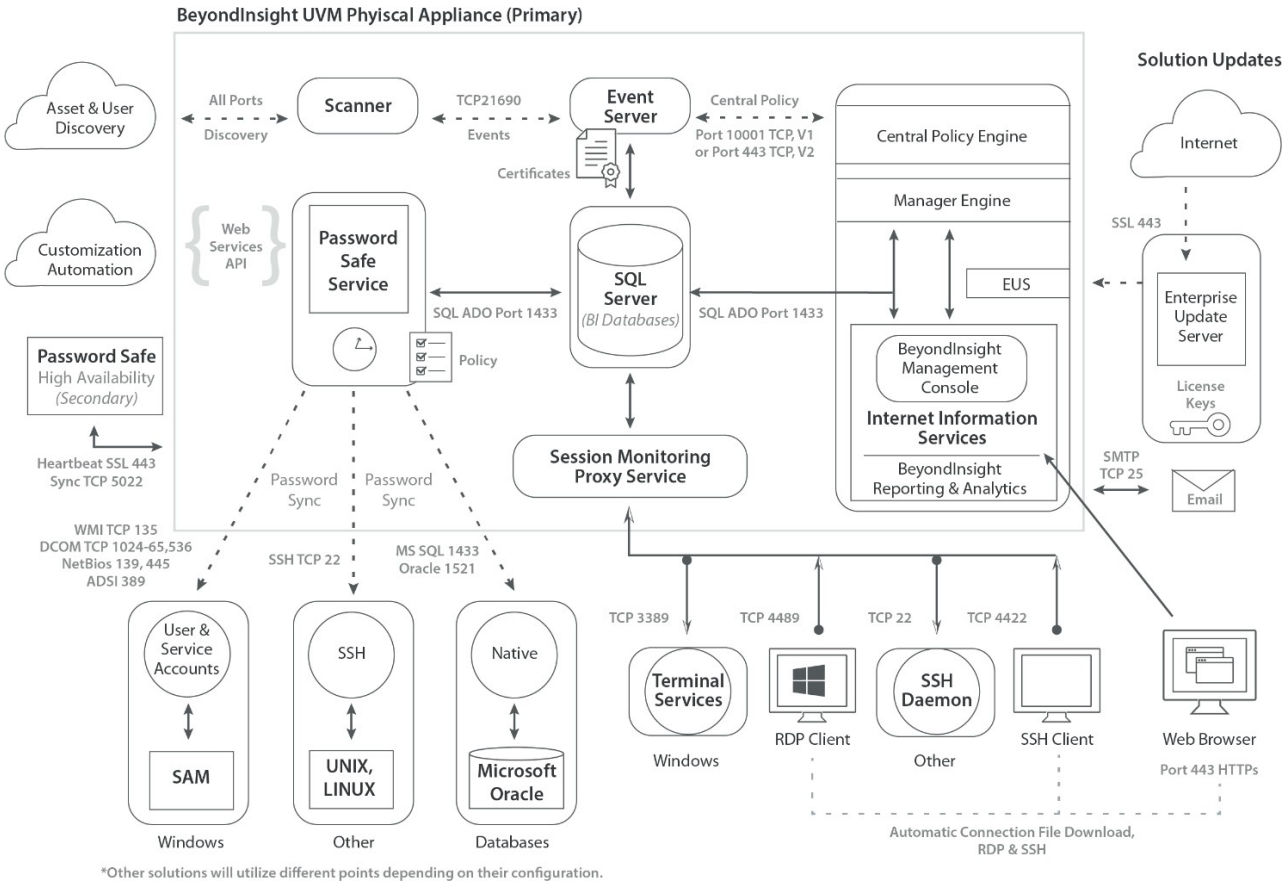
VMware vMotion can be used to keep the UVM virtual appliance continuously available even if the physical server running the virtual image goes offline for any reason. As seen above, the UVM virtual image is deployed to ESX Server X. This server is continuously mirrored to Server Y such that if a hardware failure were to occur, the virtual image continues to be available as if nothing happened.

BeyondInsight

Password Safe is part of BeyondTrust's BeyondInsight platform. The high level BeyondInsight architecture is designed to centrally manage all BeyondTrust's solutions.



Password Safe Architecture



Password Safe Scalability

NOTE: Figures on UVMv20 assume memory and CPU are at maximum (32GB RAM and 2/4 CPU).

Appliance	Max Managed Accounts	Max Concurrent Sessions
UVM20 (Physical)	30,000	300
UVMv20 (Virtual)	30,000	300
UVM50 (Physical)	250,000	600

Deployment Methodology for DR

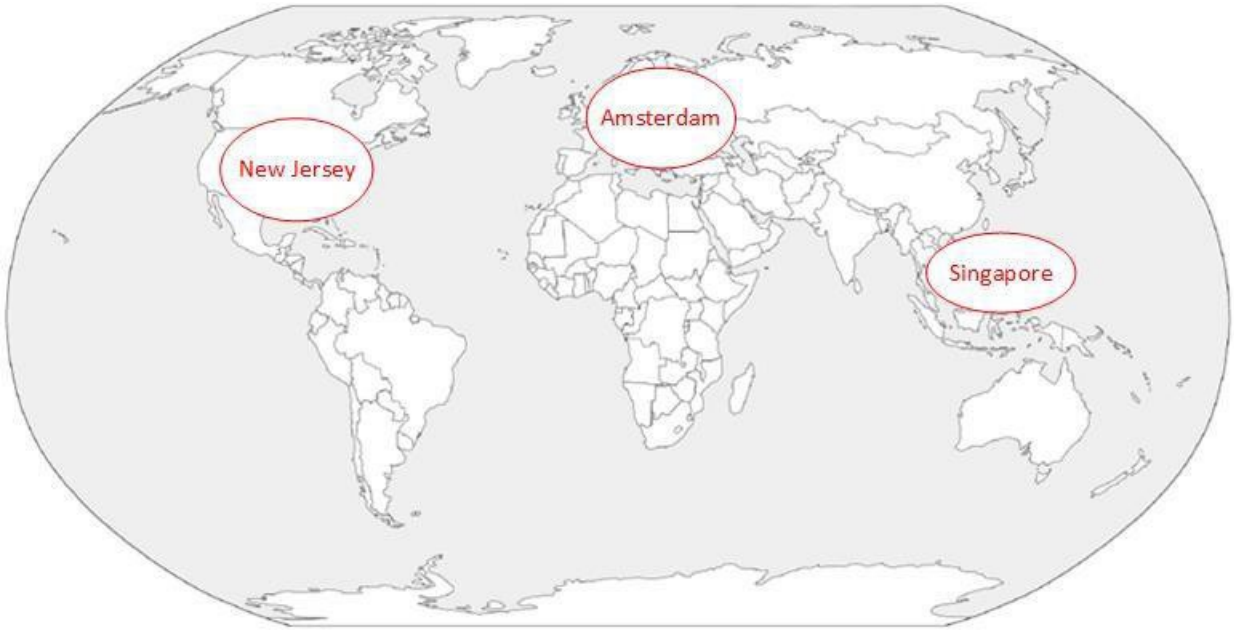
BeyondTrust Password Safe can be deployed in many different configurations to scale from single site installations to multi-site, geographically dispersed environments. The outline for this document will be based on a multi-site active/active deployment using appliances.

In an active/active deployment, appliances (or software) contain all components necessary to deploy the solution including SQL Server database, Scanner, BeyondInsight, and UVM appliance management components (backup/HA/appliance administration etc).

Microsoft SQL Server 2014 AlwaysOn Availability Groups may consist of a primary replica, and up to 8 secondary replicas in either synchronous-commit or asynchronous-commit mode. Replicas are also supported in both Azure and AWS environments; a typical deployment model comprising an asynchronous replica in the Cloud provides access to password data in the event that all on-prem components become unavailable.

SQL Server has a single master model, therefore only one replica will have write access at any one time; however, replicas may be located in multiple locations for the event of database failover.

The DR Scenario Environment

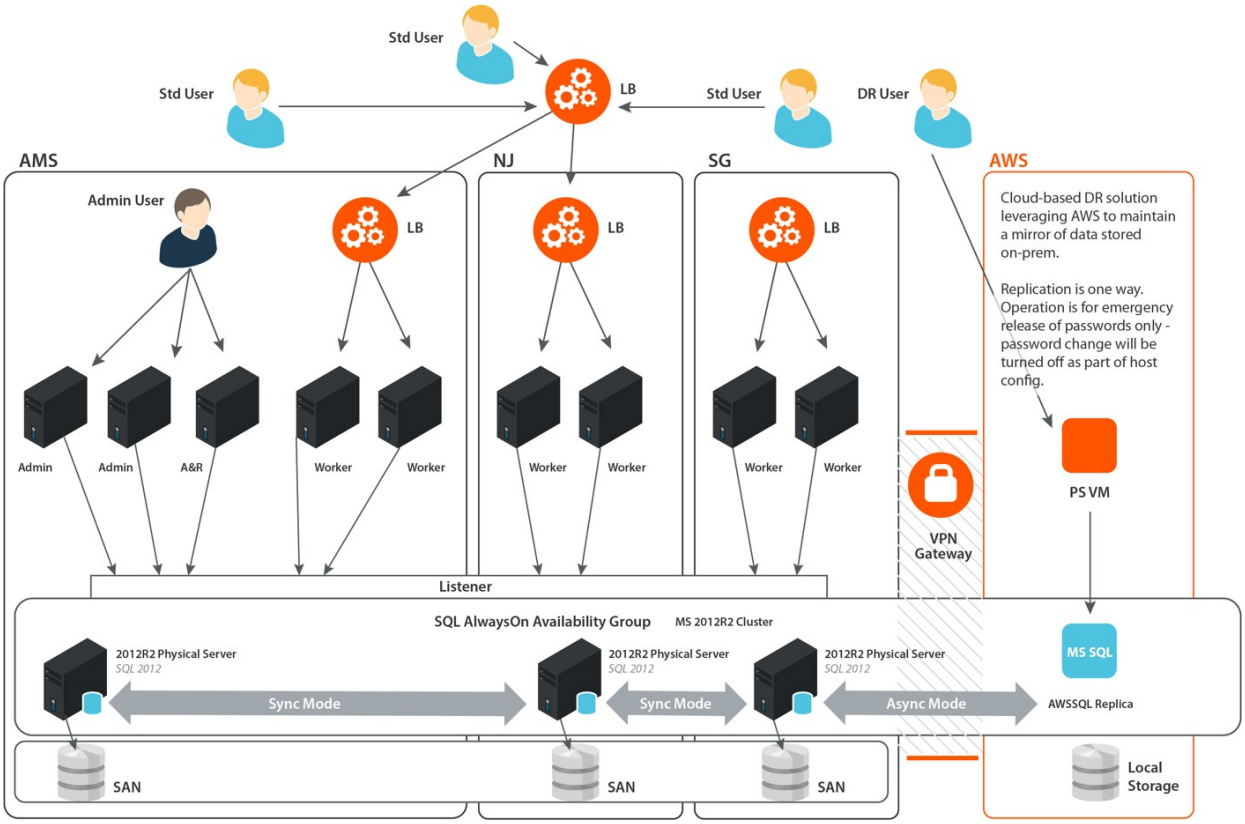


The active/active scenario has three primary sites:

- Amsterdam
- New Jersey
- Singapore

DR Active/Active Primary-Sites Deployment

Example DR Component Layout



In this example, UVM appliances in each of the three primary datacenters Amsterdam, New Jersey, and Singapore, are connected to a MS SQL AlwaysOn Availability Group. Note that each appliance can initially assume any mix of roles and may be reconfigured at any time after deploying into production.

This example contains appliances that have been configured for the following roles:

UVM – Admin Node

- Admin Management
- Admin Console
- Password Portal
- DiscoveryScanner
- Session Recording
- Password Management

UVM – A&R Node

- Analytics
- A&R Db
- SSIS
- SSAS
- SSRS

UVM – Worker Node

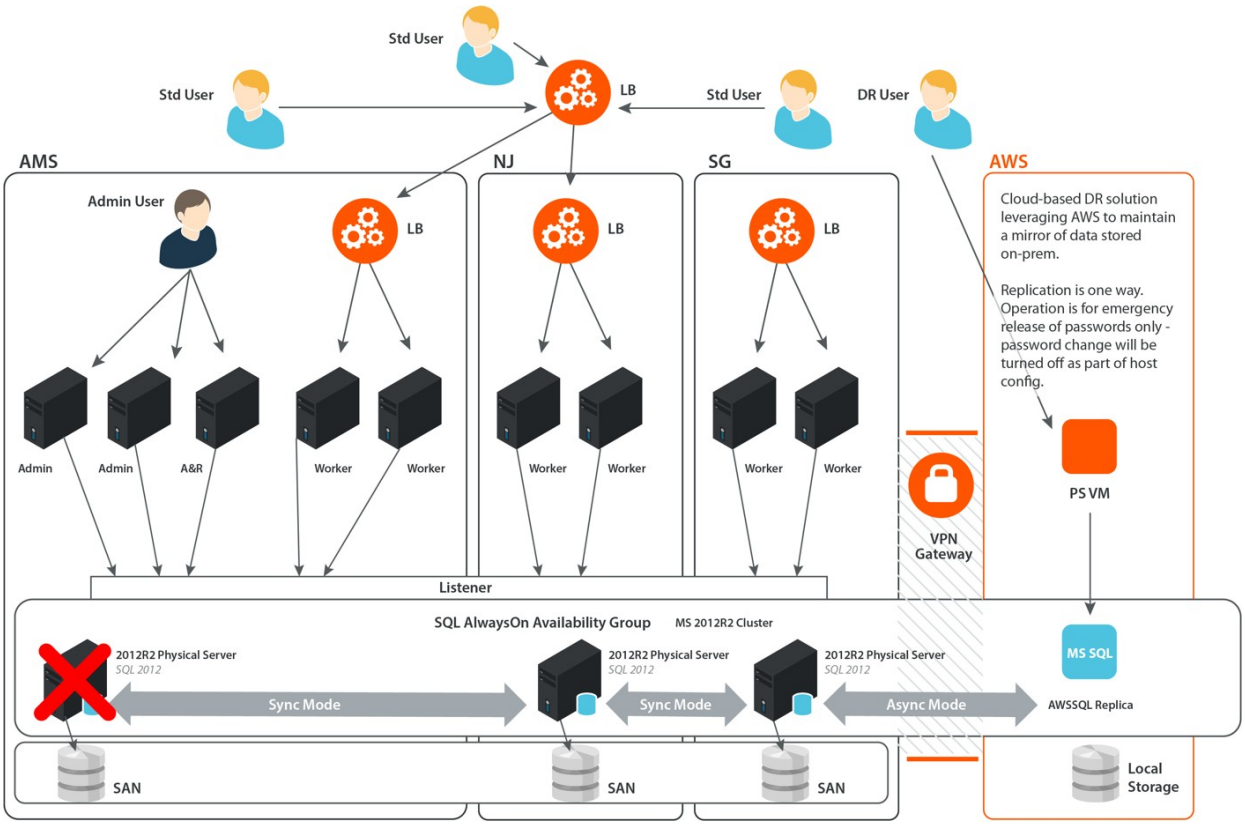
- Discovery Scanner
- Password Portal
- Session Recording
- Password Management

It can be seen that many more appliances can be added, each with varying roles: Scanners; Event Servers; Password Portals, Session Managers; Password Management. Behind load balancers, appliances may be added for redundancy, and scalability; for example, session managers configured to send recordings to archive servers can be brought down with no loss of data or functionality. As many appliances may be added as required and pointed at the availability group. Note that only one admin (manager) service is supported at any one time but this may be configured to failover to a secondary appliance.

Microsoft SQL AlwaysOn Availability Groups may consist of a primary replica, and up to 4 secondary replicas in either synchronous-commit or asynchronous-commit mode. Replicas are supported in both Azure and AWS environments; a typical deployment model comprising an asynchronous replica in the Cloud provides access to password data in the event that all on-prem components become unavailable.

In this example, an additional async commit replica has been added in a cloud environment (AWS or Azure) to provide DR capability. BeyondTrust has an AMI UVM available now https://aws.amazon.com/marketplace/pp/B01LX1SID6 , and an Azure appliance.

DR Primary Sites Scenario 1 – Loss of a database server



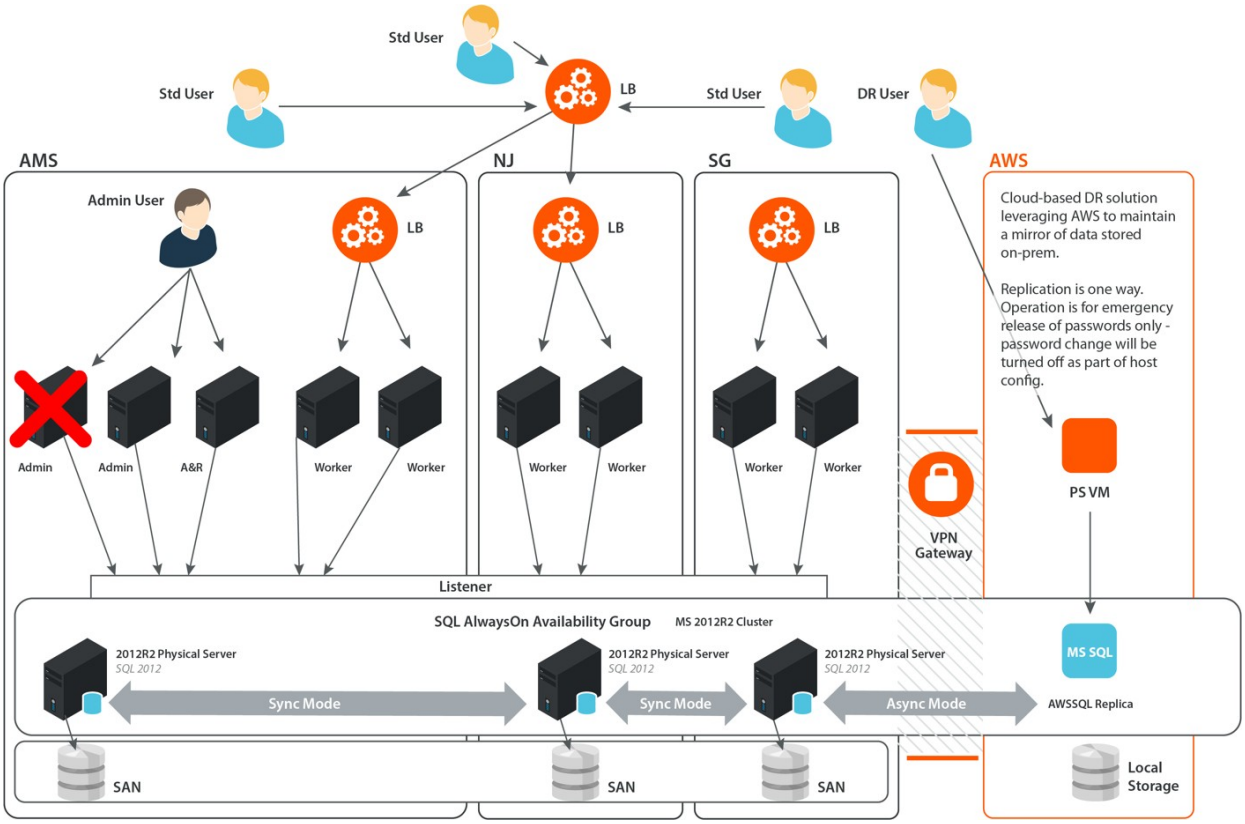
For an environment using SQL Always On, a minimum of 2 synchronous-commit replicas are assumed. In the event that the replica holding the primary role fails, the secondary replica may be set to automatically (or manually) become the new primary. In general use, secondary replicas are used for redundancy only; all read/write database operations are handled by the primary replica. In the event that a local listener is unavailable, UVMs may be easily configured to point to an alternate database listener.

A more comprehensive set of failover scenarios are covered here:

https://msdn.microsoft.com/en-us/library/hh510230.aspx

For catastrophic failure of all database components it will be necessary to restore from an offline backup of the database to a secondary or tertiary data center.

DR Primary Sites Scenario 2 – Loss of the Admin UVM



Administrative procedures such as configuring Smart Rules, permissions, and onboarding systems, accounts, and users are performed using the BeyondInsight user interface.

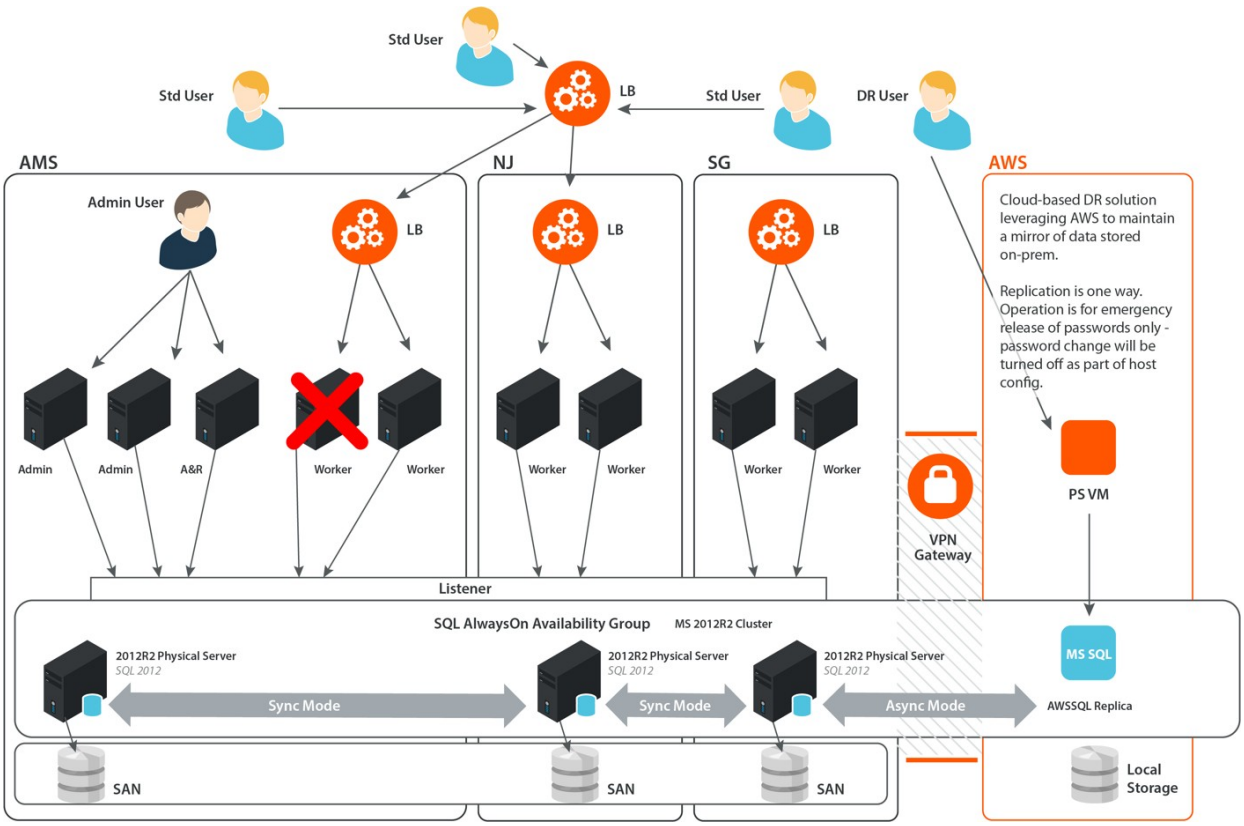
There can only be one node running the BeyondInsight interface at one time due to potential contention between more than one Manager Service.

UVM appliances have multiple Roles that may be configured at any time. If a UVM running the Admin Role fails, or is brought offline, an alternate UVM may be configured with the Admin Role. It is recommended, as in the above diagram, to have a secondary node of similar specification that the Admin Role can be switched over to.

Loss of a node running an Admin Role does not affect the operation of any other UVM, including Worker nodes, or Analytics & Reporting nodes.

Smart Rule operations are executed by nodes running the Admin Role, thus auto-onboarding, and other Smart Rule actions will be affected if no Admin Node is available; However, any scheduled password changes that have already been added to the central database queue will continue to be serviced by the Worker nodes, and any end user-based request operations will be unaffected.

DR Primary Sites Scenario 3 – Loss of a Worker UVM



UVM appliances connect independently to the database and contain the web interfaces and processes that allow end users to interoperate with the solution. Typical use case scenarios are:

- User - Requesting a new password release or RDP/SSH session
- Admin - Approving user requests
- Admin - Monitoring and remote control of user session activity
- Admin/Auditor - Search and replay of user sessions

In the event that a UVM fails or becomes unavailable for any reason (network outage, etc.), the user may be automatically re-directed via load balancer to an alternate UVM configured with similar roles.

In the example shown above, the 'Workers' are configured with the following roles:

Discovery Scanner

Scanners are given specific jobs to action. If an alternate scanner is configured, the job will be resubmitted on next job execution.

Password Portal

Users that are logged in when loss of service occurs will be redirected via load balancer to an alternate UVM. Depending on SSO authentication technologies implemented, the user may or may not be prompted for a password on failover. Given that the user's browser will be connecting to the VIP/listener of the load balancer, the user should be re-directed to the same session they were in when the failover event happened.

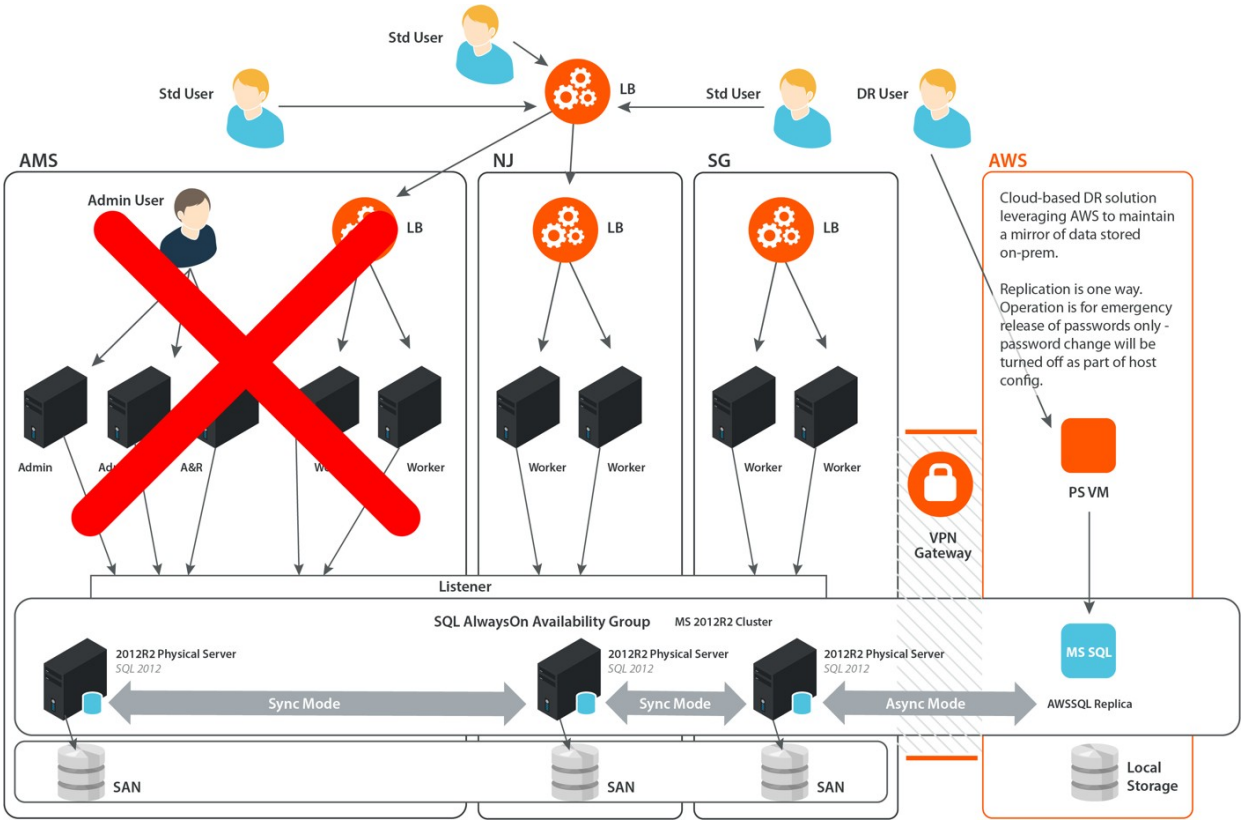
Session Recording (proxy)

Any sessions that are in process will be halted. When the user is redirected to an alternate proxy, a new RDP/SSH/Application session will be established with their target host. If the failover event is catastrophic, and the original UVM is unrecoverable, any session video recording files that were in process when the event occurred will be lost. To safeguard historical recordings, it is recommended to implement an archive server 'zero-retention' strategy as below. Keystrokes (if applicable) are sent to the database directly and are largely not affected.

Password Management Queue Agent

If a password management queue agent becomes unavailable, an alternate agent will continue to service password requests / messages from the central database queue. Queue Agents may be configured such that they will service only requests for specific groups of accounts. In this manner, loss of an agent in New Jersey will result in the alternate New Jersey agent taking over the request processing.

DR Primary Sites Scenario 4 – Loss of the primary site



If the primary site containing read/write database replicas were to go offline, the following actions should be observed/taken:

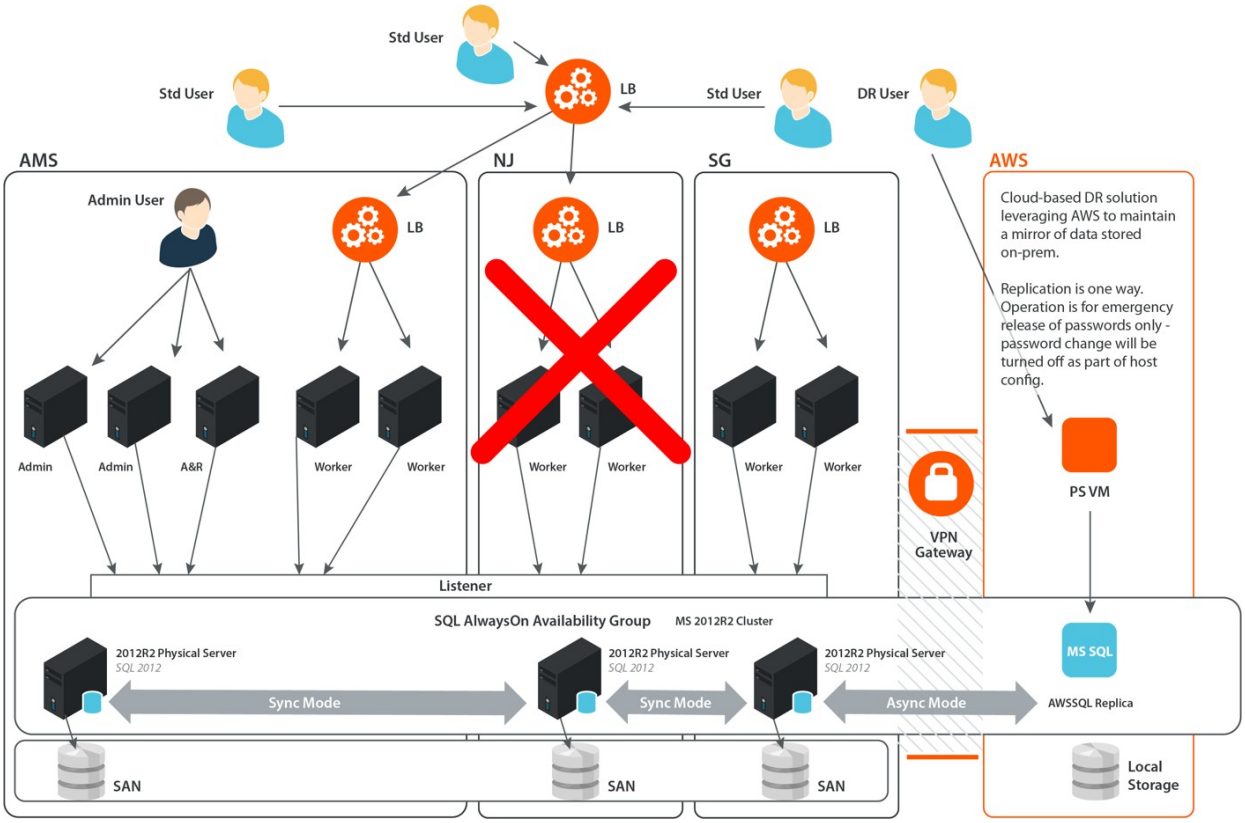
1. Failover of the primary instance to a synchronous-commit instance in the secondary datacenter –
   configured per Microsoft best practices, this may be a manual or automatic failover.

2. Manual Role configuration of the UVM appliances in the secondary datacenter to provide at least one Admin Role (for Smart Rule processing and system configuration).

3. Depending on SSRS configuration (location of reporting database), the Reporting Role should be enabled on an alternate UVM, or the reporting database restored to a backup appliance

4. Users should automatically be redirected to an alternate UVM portal via load balancers.

DR Primary Sites Scenario 5 – Loss of a secondary site

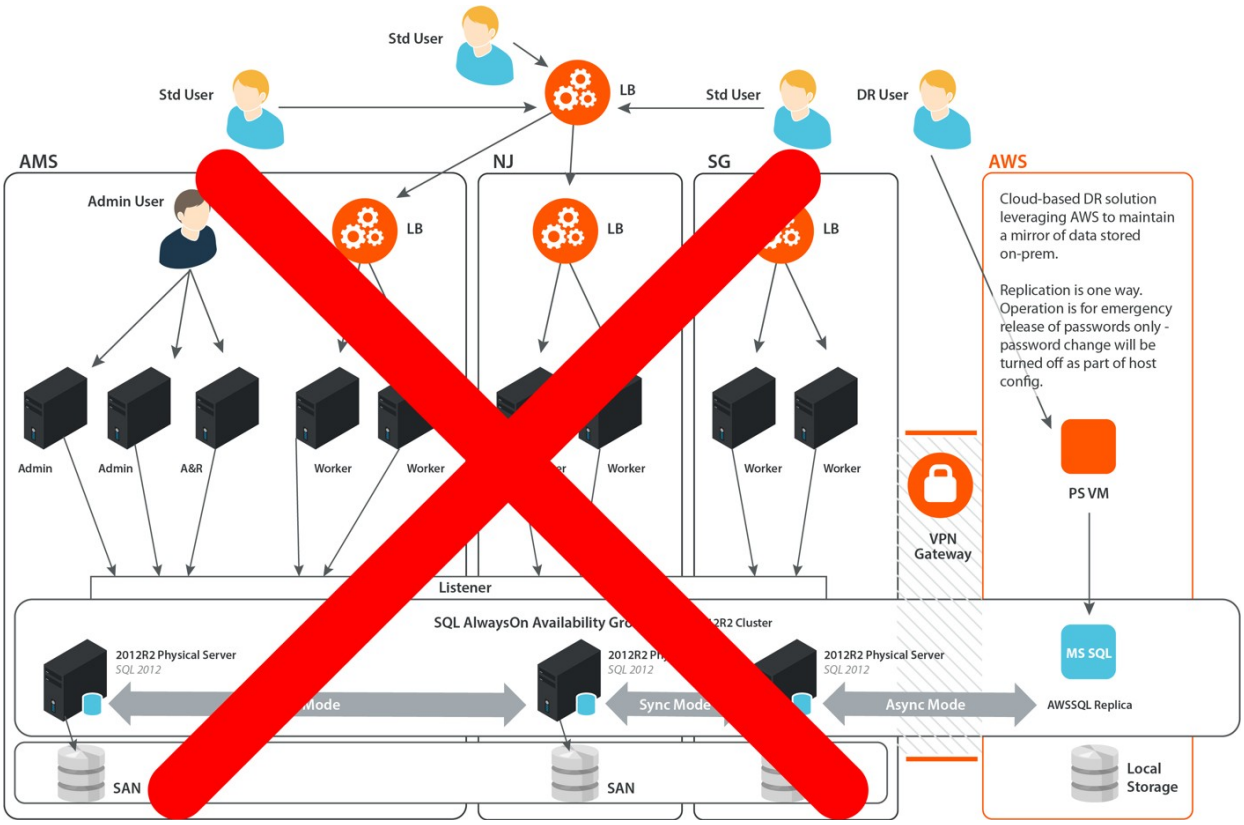


In the event that a secondary site were to go offline, users would be automatically re-directed by the load balancers to either one of the alternate sites in operation.

In this instance, no Role configuration is required.

For longer term outages, it may be necessary to modify the Workgroups of any managed accounts previously serviced by UVMs in the site that suffered an outage, such that those password change events may be serviced by UVMs from the alternate sites.

DR Primary Sites Scenario 6 – Loss of access to all on prem infrastructure



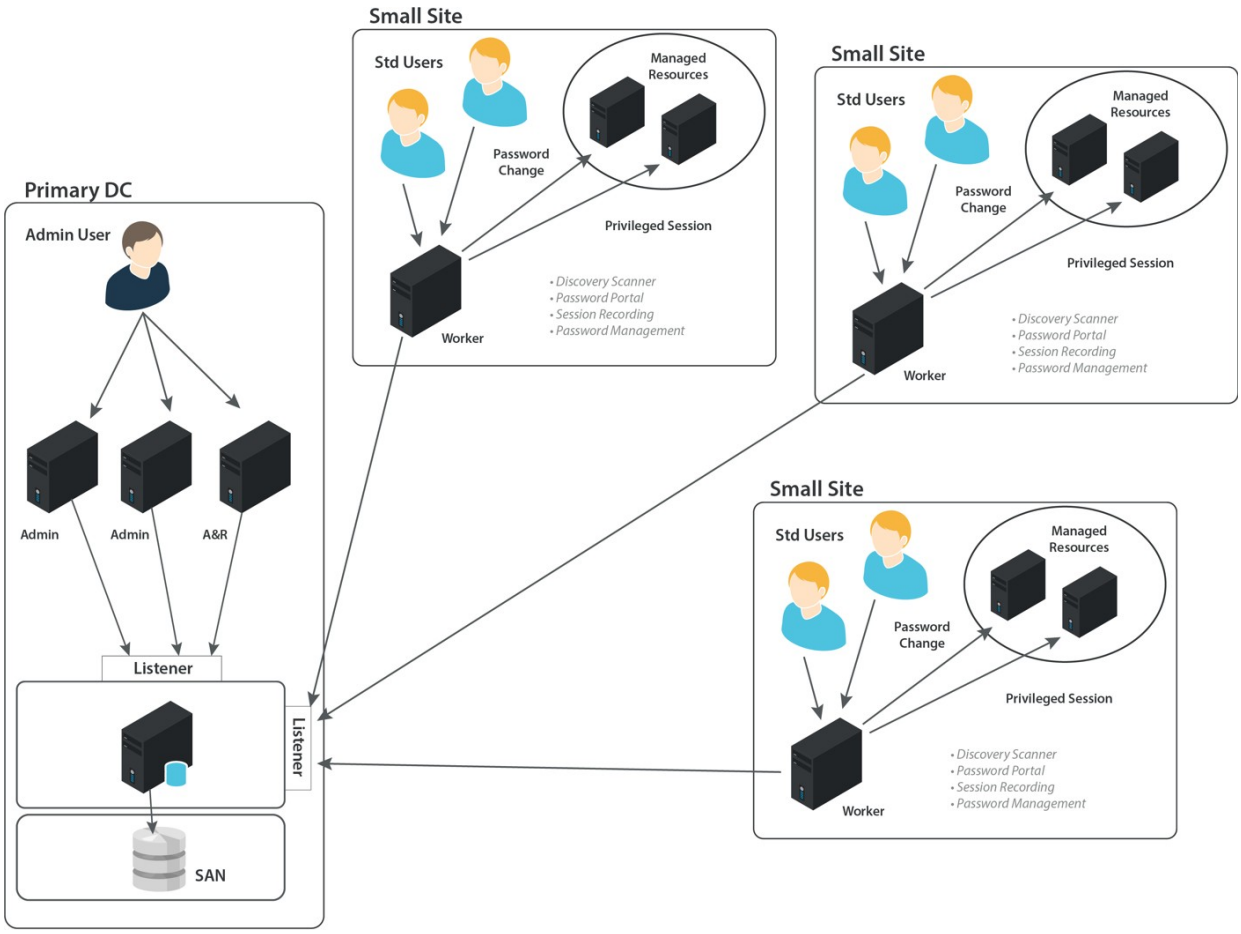
If access to all on premise systems were affected, the following methodologies should be taken into consideration

1. Short-term outage – Passwords may be retrieved via AWS (or Azure) environment. In this event, emergency access to Password Safe may require release of passwords manually stored in physical safes.

2. Longer-term outage – database restoration and key UVM appliance restoration into tertiary data centers. Note that UVM backups contain all settings and encryption keys (not applicable if using external HSM). For DR environments, consideration must be given to host naming, IP address conflicts, domain name resolution, and firewall rules. It is also important to consider such questions do you care about password rotation in a DR scenario, or can you wait until you have recovered?

This document is not intended to be a detailed blueprint of data center DR best practices but instead highlighting where PAM needs to be considered. Layers of redundancy will always mitigate a DR event but often it always comes back to that highest authority. For the system-super-user with access to all credentials in Password Safe - the ultimate break-glass may sometimes be to have a password written on a piece of paper in a vault.

DR Small-Sites Deployment



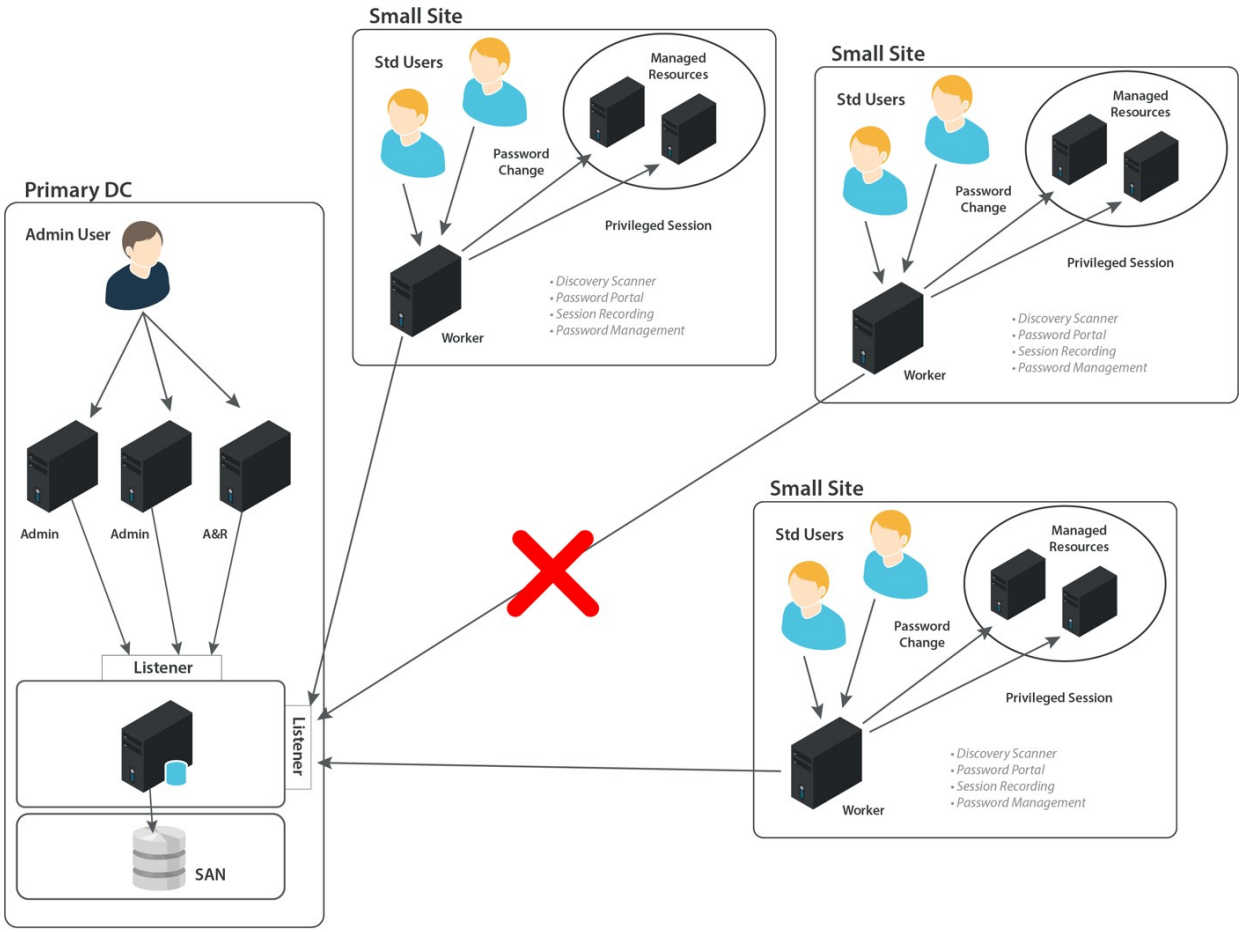
node is configured with a Workgroup name specific to the site; all managed accounts on the site are configured with the same Workgroup. In this manner each Worker node would be responsible for changing just the passwords for the site it is located in.

End users log on to the Worker node to perform the following actions:

- User - Requesting a new password release or RDP/SSH session
- Admin - Approving user requests
- Admin - Monitoring and remote control of user session activity
- Admin/Auditor - Search and replay of user sessions

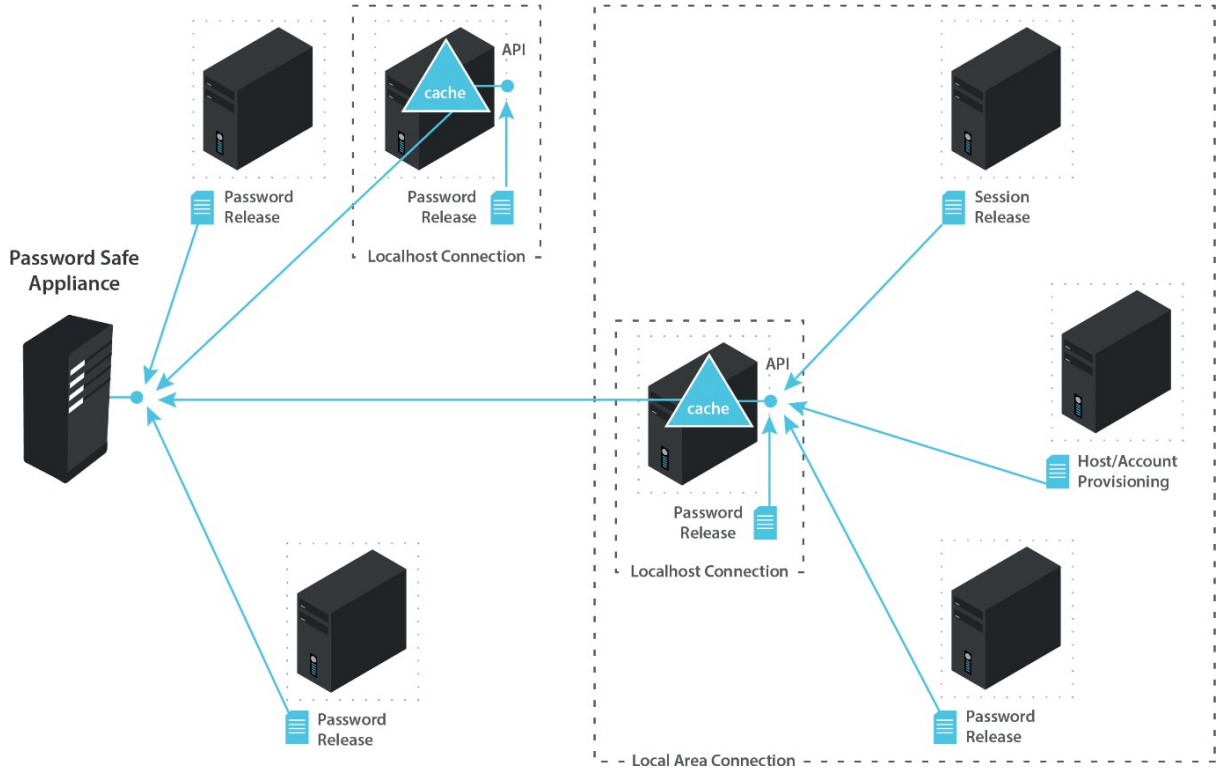
Sessions are proxied via the local Worker node; recorded keystrokes (if applicable) are stored in the central database; recorded session files may be stored locally on the node according to retention rules or transferred immediately to central archive storage locations.

DR Small Sites Scenario 1 – WAN Link from Primary Sites Down



In the current architecture, any separation from the central database will prevent users from logging on to the Worker node.

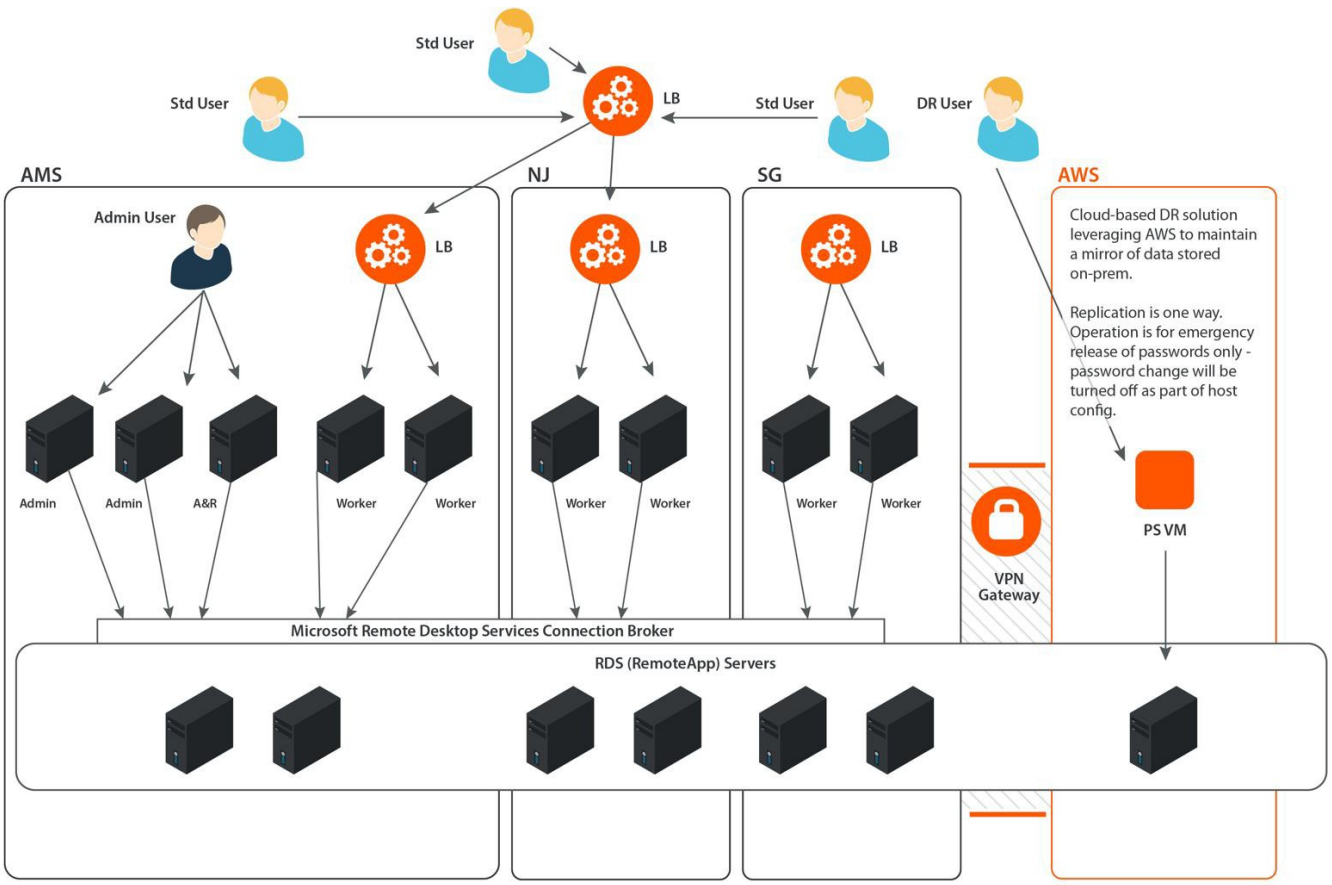
As a mitigating step, it is possible to install an unlimited number of Password Caches in the Password Safe environment to persistently store credentials in the event of an outage.



Each Cache can store credentials that may be released in an emergency. A synchronized storage option for the Worker node is planned for a future release of Password Safe.

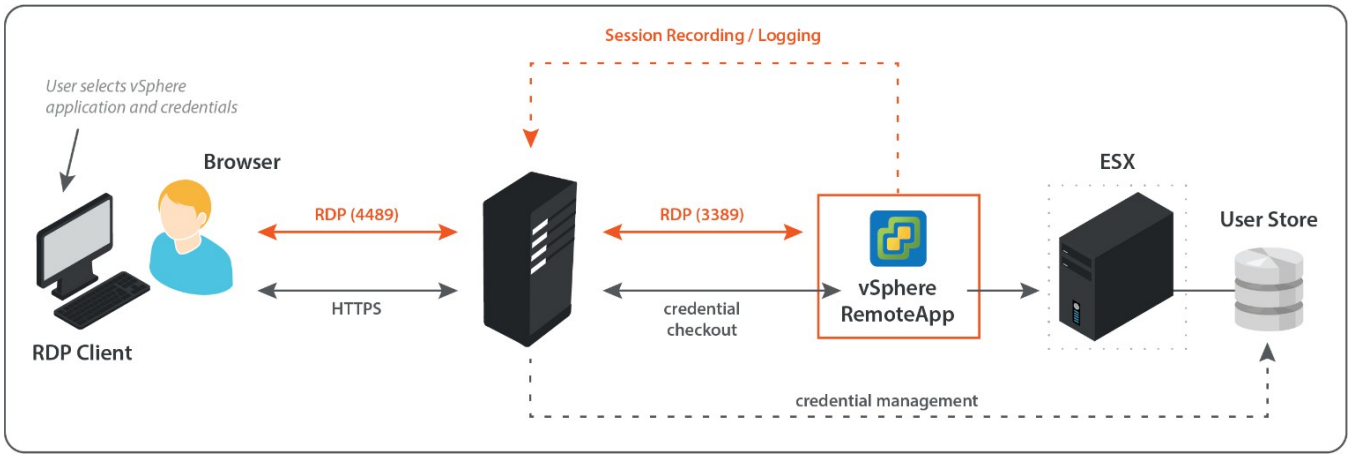
DR RemoteApps Deployment

Example RemoteApp Architecture



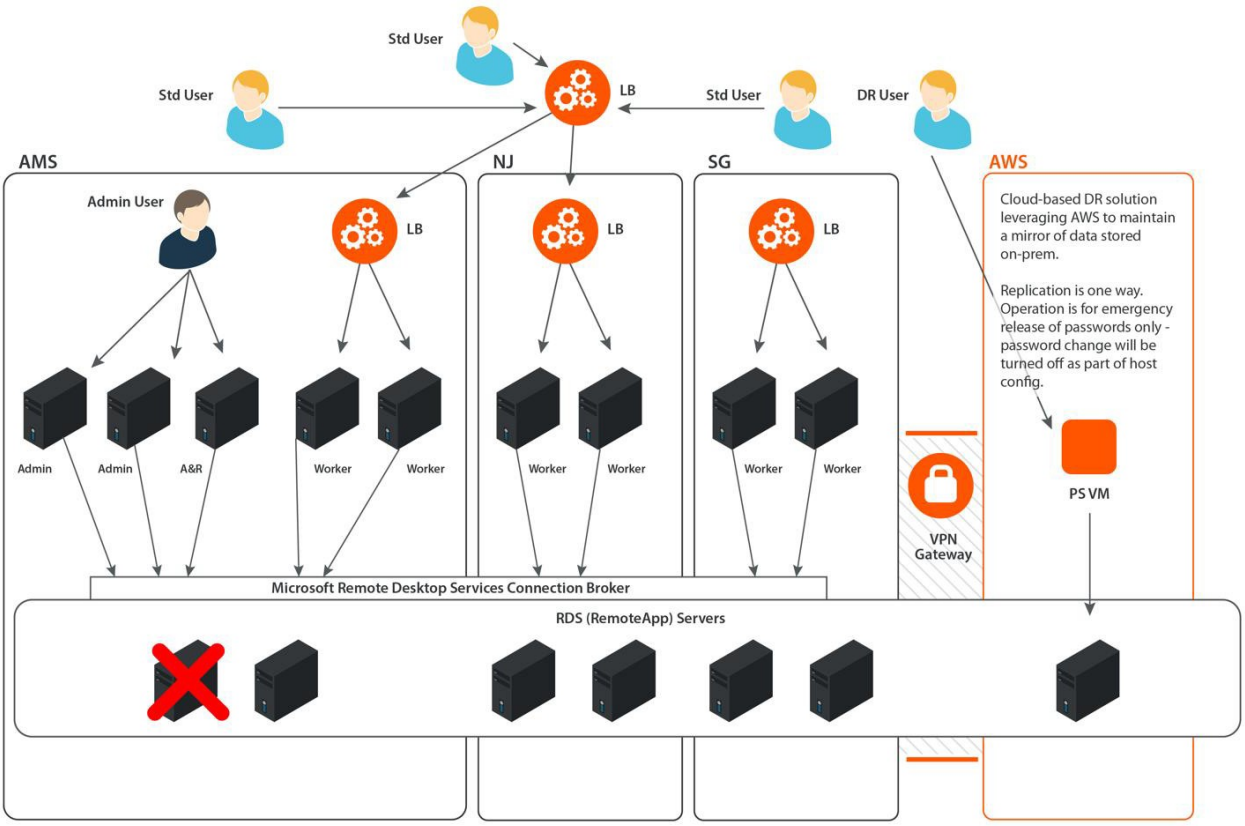
Proxy Failure Scenarios

For Windows applications and Web applications, Microsoft RemoteApp infrastructure is used to deliver applications via RDP to the end user. Passwords are played in automatically via customizable scripts.



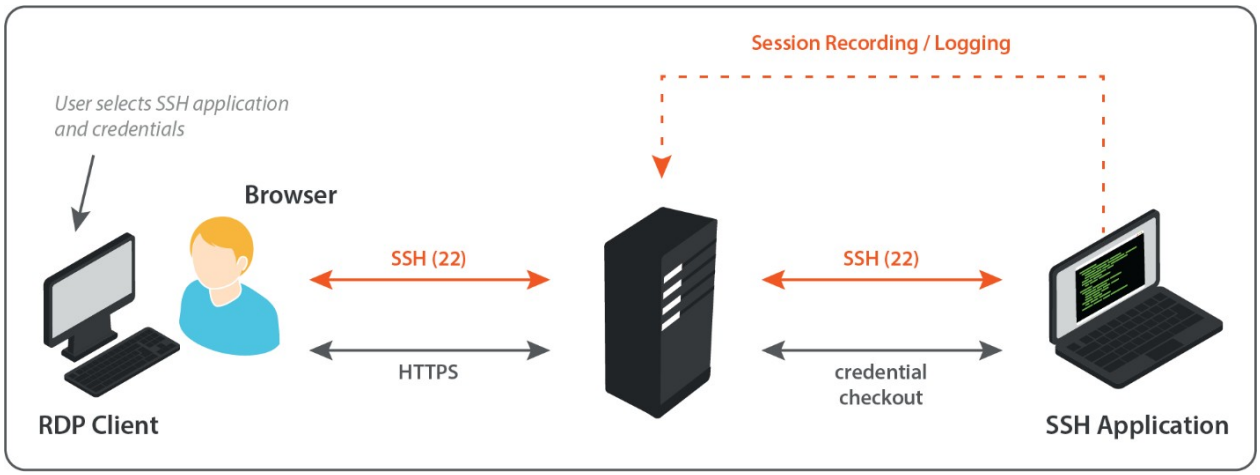
In the event of UVM/Proxy failure, the user is redirected to an alternate Worker node where they can establish a new connection using the same checked out session.

DR RemoteApp Failure Scenario



If a RemoteApp (Remote Desktop Server) were to fail, Microsoft RD Connection Brokers may be used to failover a user session to an alternate host. Another method is to add load balancers between the Session Proxy (on the Worker node), and the RemoteApp Servers.

For Unix/Linux applications, no external components are required; the Session Proxy can launch any command line tool directly through each UVM.



In the event of UVM/Proxy failure, the user would be redirected to an alternate Worker node where they can establish a new connection using the same checked out session.

Appendix – Default Ports

System Discovery

Functionality	Service	--->	Protocol	Requirement/Notes
User Enumeration	nb-ssn|ms-ds	139|445*	TCP	
Hardware Enumeration	nb-ssn|ms-ds	139|445*	TCP	WMI Service running on target
Software Enumeration	nb-ssn|ms-ds	139|445*	TCP	Remote Registry service running on target
Local Scan Services	ms-ds	445	TCP	
		* Note: 445 preferred		

Desktop Connectivity

Functionality	Service	--->	Protocol	Requirement/Notes
User interface	https	443	TCP	
Remote Desktop	rdp	4489	TCP	
SSH	ssh	4422	TCP	

Network Devices

Functionality	Service	--->	Protocol	Requirement/Notes
Checkpoint	ssh	22	TCP	
Cisco	ssh	22	TCP	
Dell iDRAC	ssh	22	TCP	
F5 BIG IP	ssh	22	TCP	
HP Comware	ssh	22	TCP	
HP iLo	ssh	22	TCP	
Juniper	ssh	22	TCP	
Palo Alto	ssh	22	TCP	
Fortinet	ssh	22	TCP	
SonicWall	Ssh	22	TCP	

Operating Systems

Functionality	Service	--->	Protocol	Requirement/Notes
AIX	ssh	22	TCP	
HP-UX	ssh	22	TCP	
IBMi (AS400)	telnet	23	TCP	
Linux	ssh	22	TCP	
MAC OSX	ssh	22	TCP	
Solaris	ssh	22	TCP	
Windows Desktop	adsi-ldap	389	TCP	ms-ds (445/TCP) is used as a fallback
Windows Server	adsi-ldap	389	TCP	ms-ds (445/TCP) is used as a fallback
Windows Update/Restart Services	wmi	135	TCP	WMI Service running on target

Directories

Functionality	Service	--->	Protocol	Requirement/Notes
Active Directory	adsi-ldap	389	TCP	ms-ds (445/TCP) is used as a fallback
RACF	ssh	22	TCP	
LDAP/S	ldap	389	TCP	

Databases

Functionality	Service	--->	Protocol	Requirement/Notes
Oracle	oracle-listener	1521	TCP	
MS SQL Server	netlib	1433	TCP	
Sybase ASE		5000	TCP	
MySQL		3306	TCP	
Teradata		1025	TCP	

Applications

Functionality	Service	--->	Protocol	Requirement/Notes
VMware vSphere API		API		
VMware vSphere SSH		22	TCP	
SAP		API		

Session Management

Functionality	Service	--->	Protocol	Requirement/Notes
Remote Desktop	rdp	3389	TCP	
SSH	ssh	22	TCP	

Appliance

Functionality	Service	--->	Protocol	Requirement/Notes
Mail Server Integration	smtp	25	TCP	
AD Integration	ldap	389	TCP	
Backup	smb	445	TCP	
Time Protocol	ntp	123	TCP	
HA Replication (pair)	sql-mirroring|https	5022|443	TCP	