BeyondTrust

BeyondInsight and Password Safe 23.3 Deployment and Failover Guide

TC:2/8/2024

Table of Contents

Password Safe Deployment and Failover Guide

Password Safe is your privileged access management solution to ensure your resources are protected from insider threats. It combines privileged password and session management to discover, manage, and audit all privileged credential activity.

Password Safe creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system.

Password Safe's random password generator algorithm does not use any common phrases or dictionary words as inputs or in its generation. It selects each password character randomly from the list of allowable characters, numerals, and symbols to build the password.

Password Safe is supported on a hardened U-Series Appliance that creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system.

More specifically, you can use Password Safe to accomplish the following:

1. Scan, identify, and profile all assets for automated Password Safe management, ensuring no credentials are left unmanaged.
2. Control privileged user accounts, applications, SSH keys, cloud admin accounts, RPA accounts, and more.
3. Use adaptive access control for automated evaluation of just-in-time context for authorization access requests.
4. Monitor and record live sessions in real time and pause or terminate suspicious sessions.
5. Enable a searchable audit trail for compliance and forensics, and achieve complete control and accountability over privileged accounts.
6. Restrict access to critical systems, including assets and applications, keeping them safe from potential inside threat risks.

This document describes three 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 Use Cases

The following are Disaster Recovery (DR) use cases to consider:

- In a DR scenario, do you 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 IDs to be the same as in primary?
- Does everyone have the same role in a DR Scenario?
- Do groups, systems, and deployment scenarios match?

Configurations Supported: Advantages and Disadvantages

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

Active/Active

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

Advantages

- Unlimited scalability.
- Redundancy of components.

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 U-Series 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 U-Series Appliance.
- The failover process can take 10 minutes or longer.

Single U-Series Appliance with vMotion

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

Advantages

- Cost effective HA with a single U-Series 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 Deployment Model

The Active/Active deployment model can be implemented using Physical, Virtual or cloud U-Series Appliances. It requires the use of an external Microsoft SQL Server database with Always On availability groups for data consistency and high availability.

As many U-Series Appliances as required can be configured to connect to the database. In this case, all U-Series Appliances can be used at once, and are fully redundant; if one goes down, you switch to an alternative. Always On availability groups may be configured with a mix of synchronous commit and asynchronous commit replicas to provide real-time database redundancy.

> ***Note:*** *In an Active/Active deployment, the active nodes don't need to be the same U-Series Appliance version. For example, they may be a mix of 2012 and 2016 nodes.*

> *For supported version information, please see the BeyondTrust Password Safe Supported Platforms Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/supported-platforms/index.htm.*

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 following settings:

- Place SQL data and log files on separate volumes and isolate from other applications using the same volume, if possible.
- Default collation.

> ***Note:*** *Data file size should be initialized at 300GB. This value varies according to scoping.*

- Log file size should be initialized at 30GB (vary according to scoping).
- Auto growth should be on and set to a fixed amount (we recommend 3GB) instead of a percentage (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.

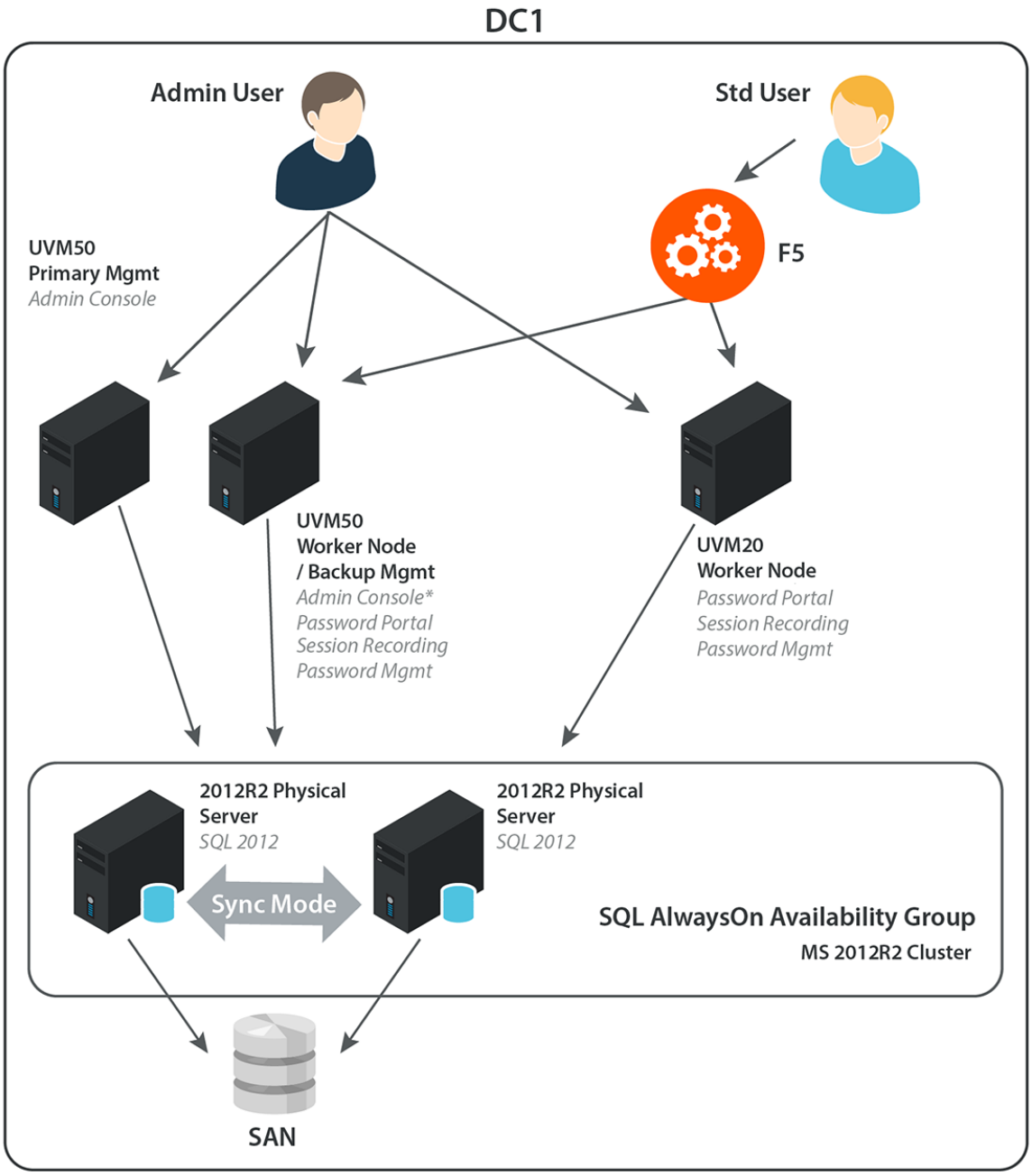
The number of nodes in the availability group will depend on customer requirements, as will the name of the nodes and listener. When creating the database during the installation process you will point to the address of the group listener. Once the database has been created you can make it available in Always On.

> *For steps on adding to Always On, please see Add a Database to an Always On availability group at https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/availability-group-add-a-database?view=sql-server-ver15.*

Single Site Deployment

A single site can contain a number of U-Series Appliances for redundancy.

In this scenario, a pair of replicas is configured for synchronous commit within an external Always On availability group. This provides database redundancy. Three U-Series 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 U-Series Appliances can be made directly or with a load balancer. Both U-Series Appliances can be used simultaneously. Session recordings are stored on the U-Series Appliance in use. Recordings may optionally be sent to a separate archive server based on disk utilization or retention.

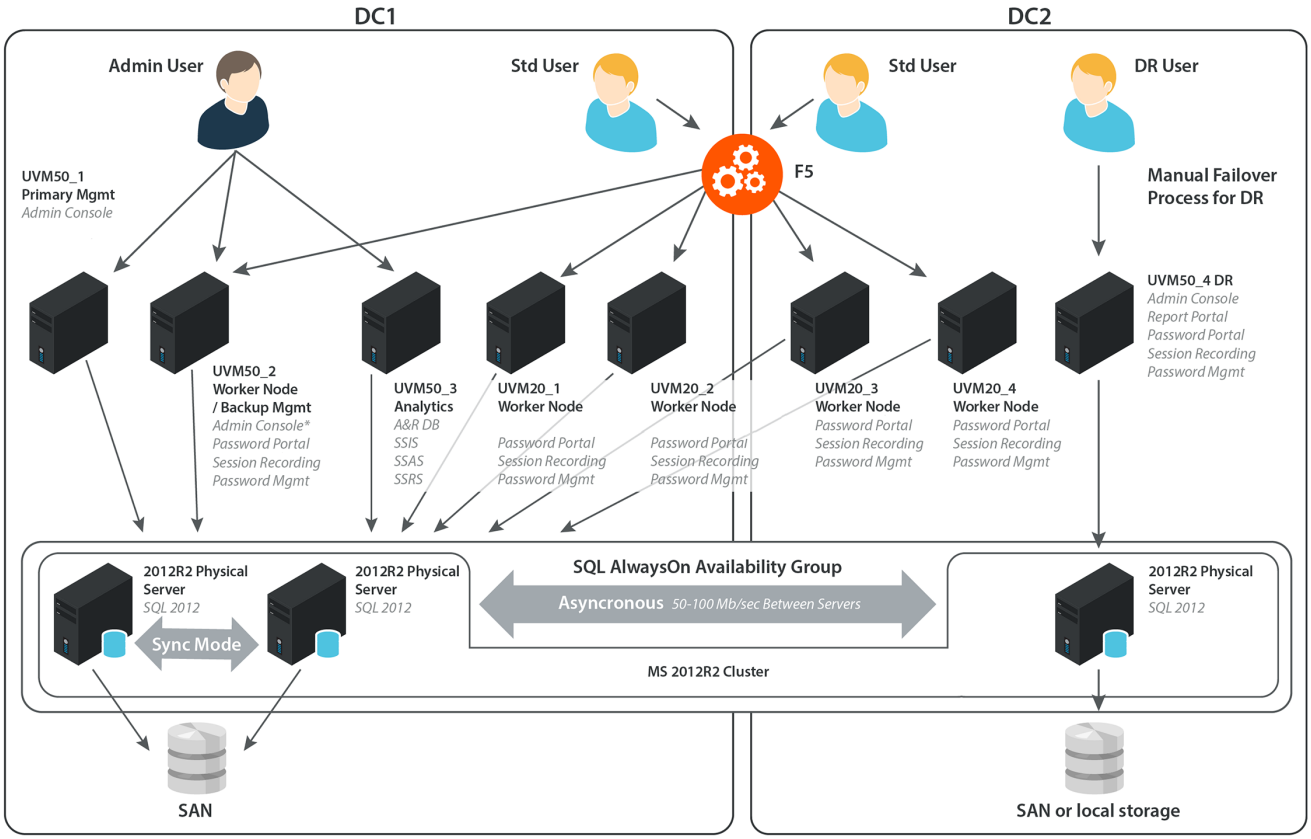


Multi-Site Deployment

In this example, multiple data centers are connected to an Always On availability group. You can see that many more U-Series Appliances can be added, each with varying roles, such as: Scanners, Event Servers, Password Portals, Session Managers, and Password Management.

Behind load balancers, U-Series Appliances can 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 disaster recovery (DR) capability. An additional U-Series 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 U-Series Appliances may be added as required, and pointed at the availability group.

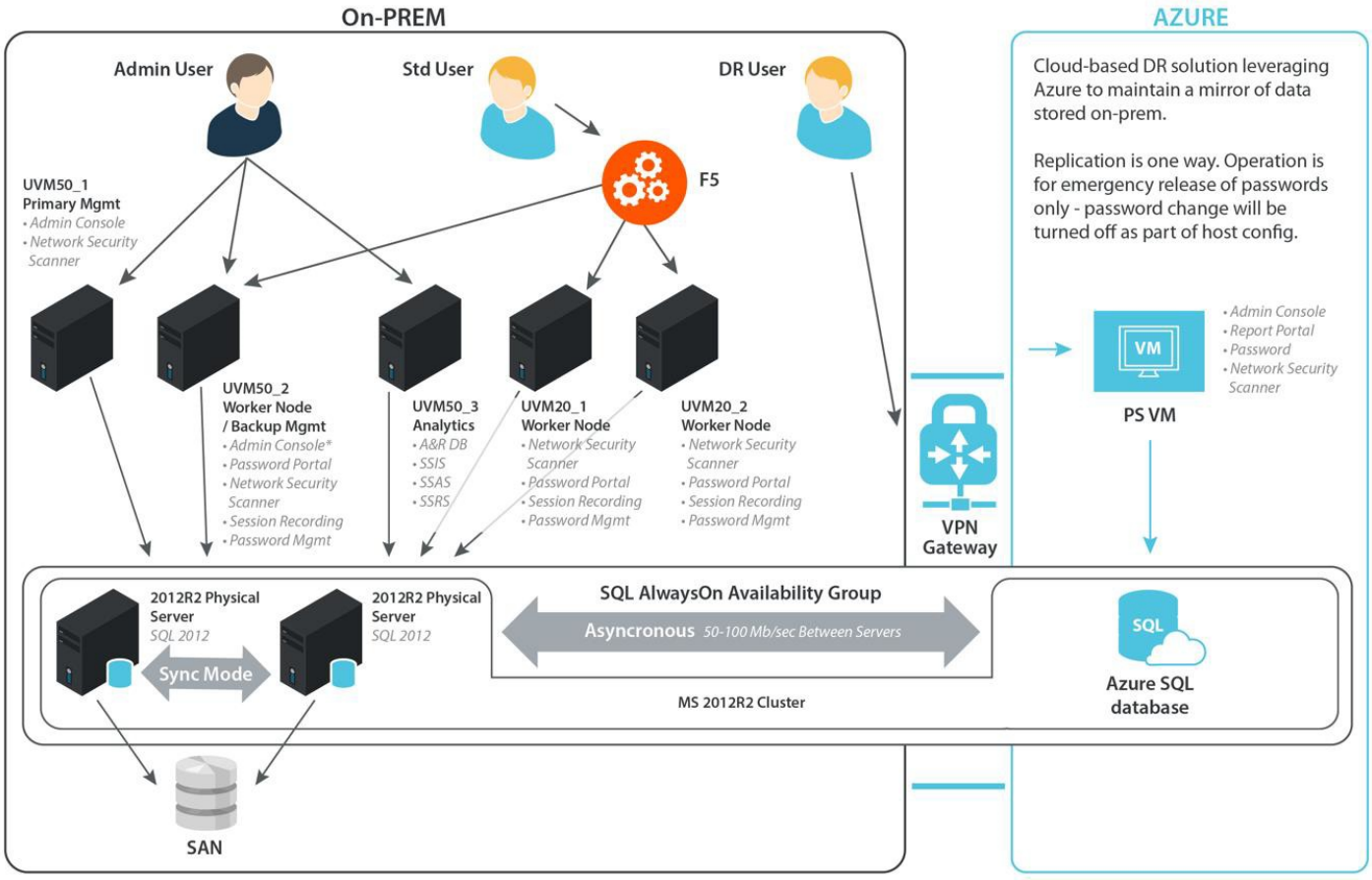
> ***Note:*** *SQL Server has a single master model; therefore, only one replica has write access at any one time. However, replicas may be located in multiple locations for the event of database failover.*



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 Always On availability groups may consist of a primary replica, and up to 8 secondary replicas in either synchronous - commit or asynchronous-commit (SQL Server 2014 and later).

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.



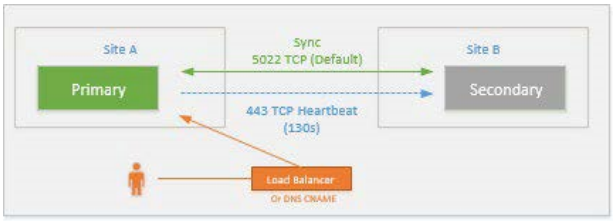
Active/Passive Deployment Model

The Active/Passive model is for U-Series Appliances only. It fails over to a mirrored U-Series Appliance in the event the primary U-Series Appliance is not available. Failover is automatic. This method involves two U-Series Appliances configured as a pair.

> ***Note:*** *U-Series Appliance pairs have to be identical i.e., U-Series 20 > U-Series 20, U-Series 50 > U-Series 50, U-Series v20 > U-Series v20.*

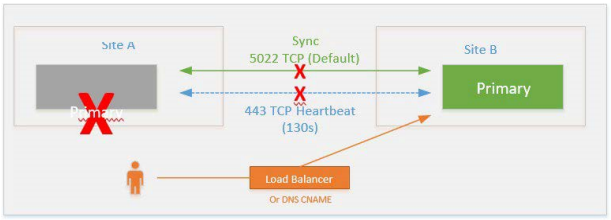
Non-Failover Stage

The database is mirrored via port 5022. A heartbeat is sent from the primary U-Series Appliance to the secondary U-Series Appliance every 130 seconds (non-configurable). If a heartbeat has not been detected for 14 minutes (default, range: 5 - 10,000 minutes), the secondary U-Series Appliance promotes itself to a primary.



Failover Stage

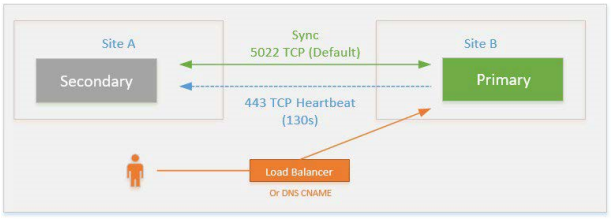
The secondary U-Series Appliance promotes itself to primary and starts servicing requests.



Recovery Stage

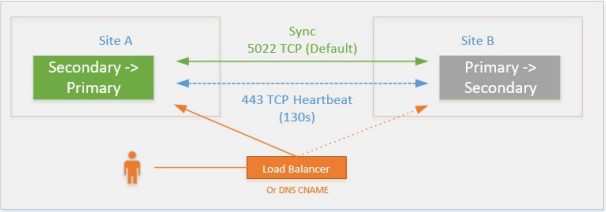
When the previous primary U-Series Appliance in Site A starts up, it looks for a replica partner. If the replica is found, the Site A U-Series Appliance starts in secondary mode, and the database is replicated from Site B.

At this point, the U-Series Appliances remain in their current roles; Site B continues to be the primary U-Series Appliance, and Site A becomes the new secondary.



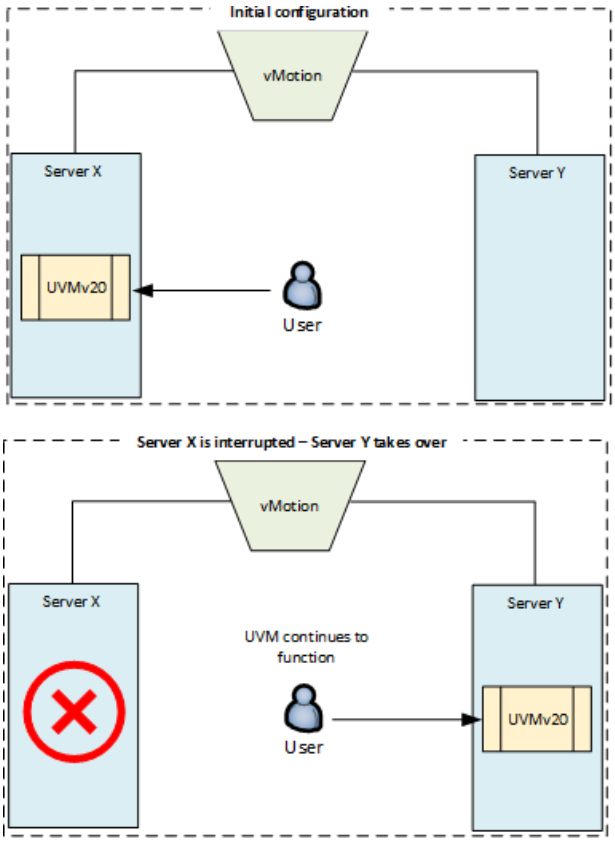
Role Reversal

If you need to revert the roles, log into either appliance and click **Swap Roles**.



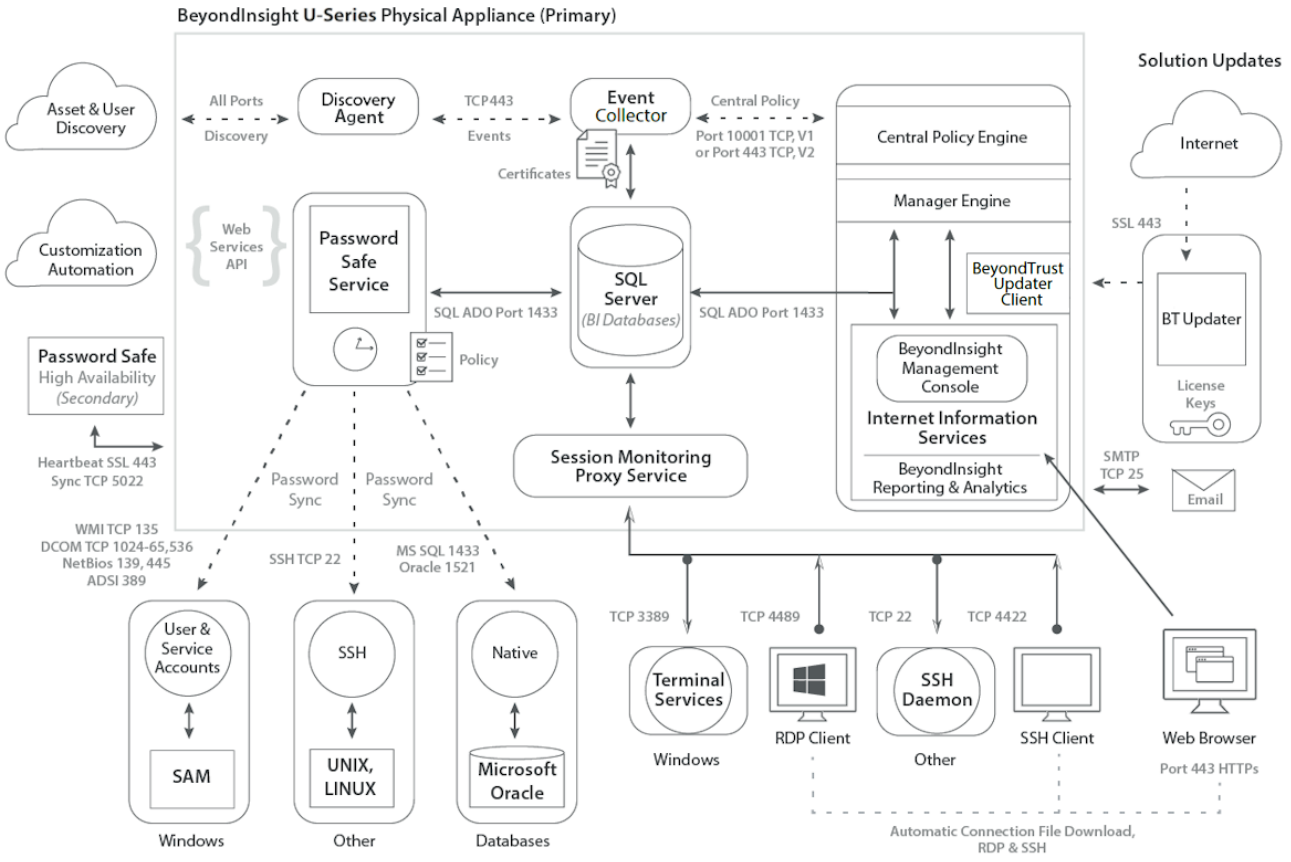
U-Series Appliance with vMotion

VMware vMotion can be used to keep the Virtual U-Series Appliance continuously available even if the physical server running the virtual image goes offline for any reason. As seen in this diagram, the U-Series Appliance 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 and Password Safe Architecture

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



> ***Note:*** *Asset and User Discovery can be configured to use any ports, but the following ports are the defaults:*
>
> - *Standard ports: 22, 80, 110, 139, 389, 443, 445, 3389*
> - *Database ports: 1025, 1433, 1521, 3306, 5000, 5432, 27017*

Password Safe Scalability

> ***Note:*** *Figures on U-Series v20 assume memory and CPU are at maximum (32GB RAM and 2/4 CPU).*

U-Series Appliance	Max Managed Accounts	Max Concurrent Sessions
U-Series 20 (Physical)	30,000	300
U-Series v20 (Virtual)	30,000	300
U-Series 50 (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. This document focuses on active/active deployment using U-Series Appliances.

In an Active/Active deployment, U-Series Appliances contain all components necessary to deploy the solution including SQL Server database, Scanner, BeyondInsight, and U-Series Appliance management components (backup/HA/U-Series Appliance administration etc).

Microsoft SQL Server 2014 Always On 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.

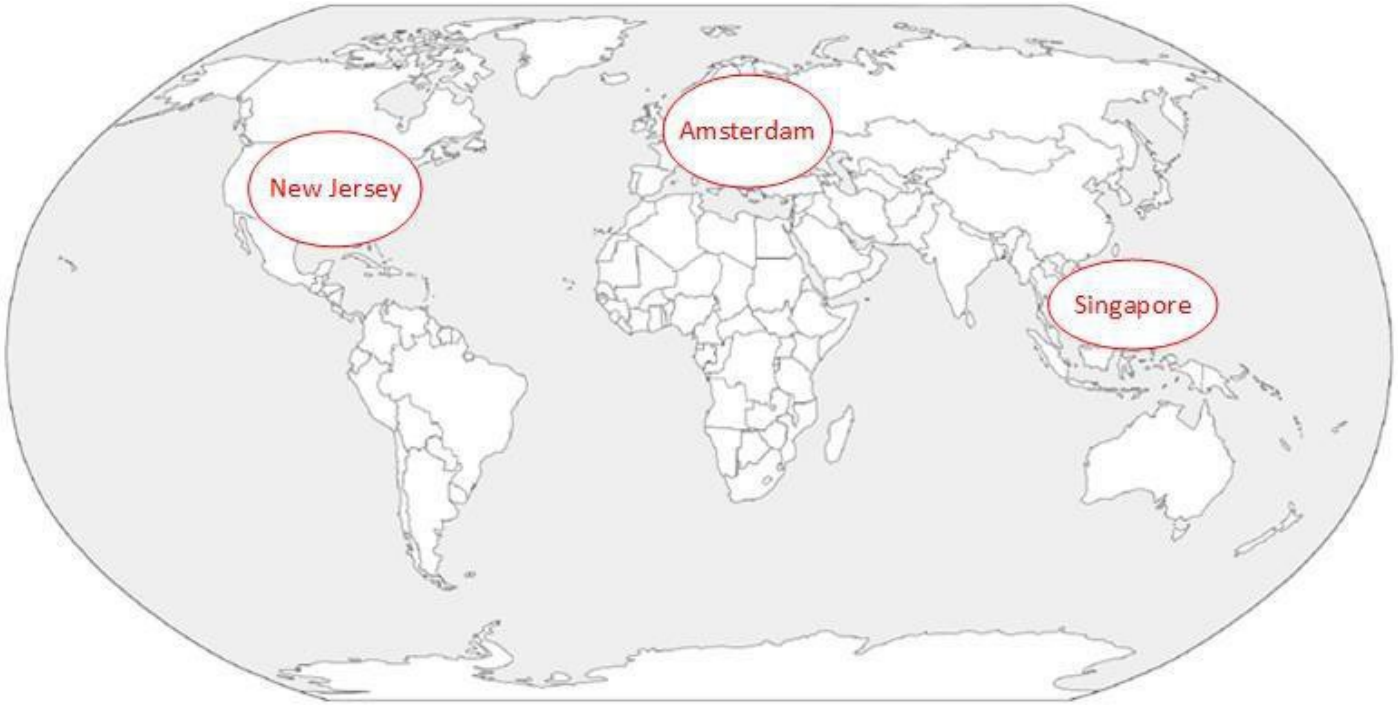
SQL Server has a single master model, therefore only one replica has write access at any one time; however, replicas may be located in multiple locations for the event of database failover.

A cold spare appliance can be connected to an active/passive cluster, as part of restoring a backup of the primary. However, by default, the restored machine is configured to be in an HA pair.

- If the DR scenario requires this machine to run independently, turn off HA.
- If the DR scenario involves restoring a second machine to pair it with, that must be set up again. The restore process does not automatically pair HA.

DR Active/Active Primary Sites Deployment

The DR Scenario Environment



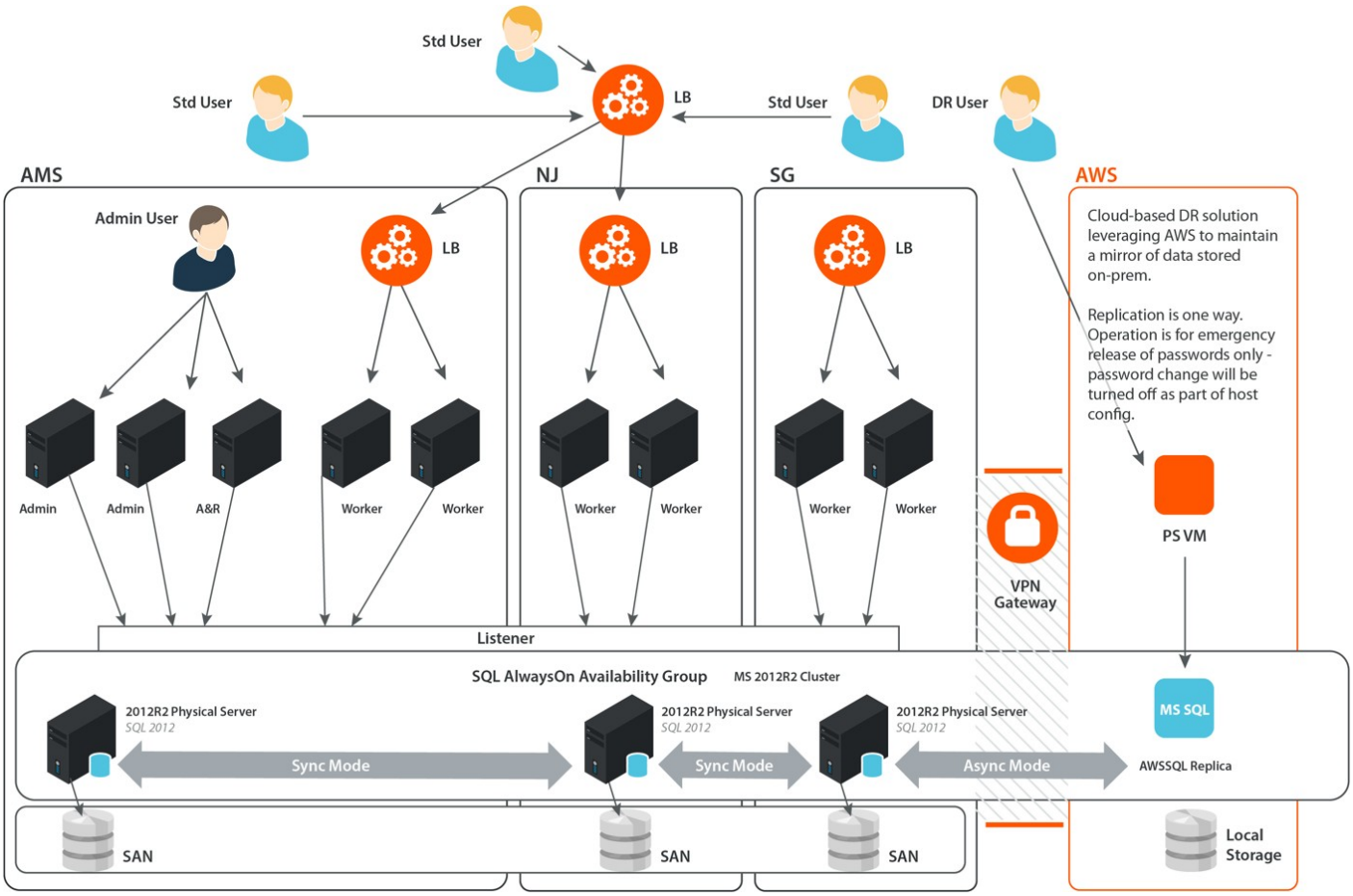
In this example, the active/active scenario has three primary sites:

- **Amsterdam**
- **New Jersey**
- **Singapore**

Example DR Component Layout

In this example, U-Series Appliances in each of the three primary datacenters Amsterdam, New Jersey, and Singapore, are connected to a MS SQL Always On Availability Group.

> ***Note:*** *Each U-Series Appliance can initially assume any mix of roles and may be reconfigured at any time after deploying into production.*



This example contains U-Series Appliances that have been configured for the following roles:

U-Series Appliance - Admin Node	U-Series Appliance - A&R Node	U-Series Appliance - Worker Node
Admin Management	Analytics	Discovery Scanner
Admin Console	A&R Db	Password Portal
Password Portal	SSIS	Session Recording
Discovery Scanner	SSAS	Password Management
Session Recording	SSRS	
Password Management		

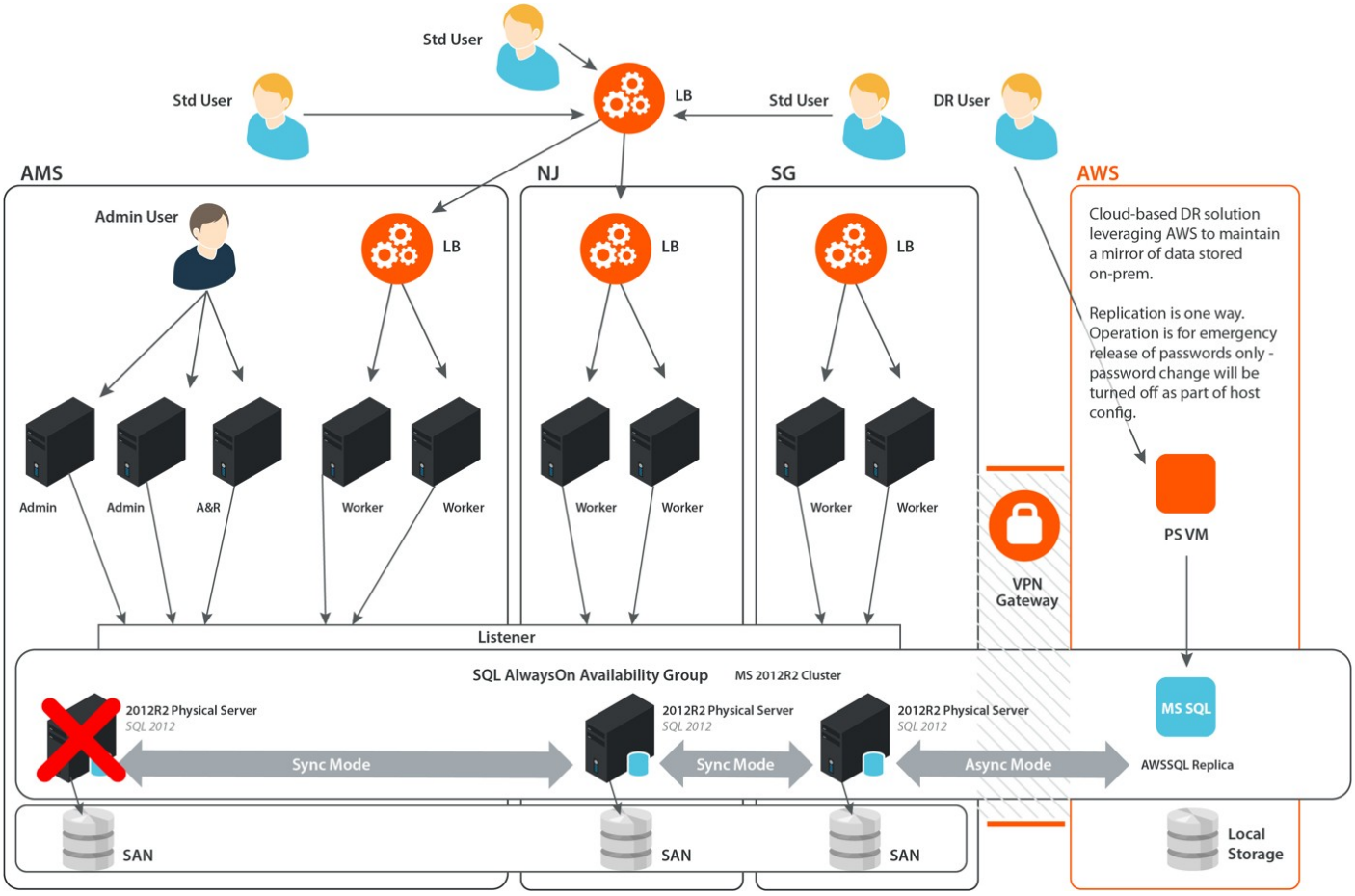
You can see that many more U-Series Appliances can be added, each with varying roles: Scanners, Event Servers, Password Portals, Session Managers, and Password Management. Behind load balancers, U-Series Appliances can be added for redundancy and scalability. For example, session managers configured to send recordings to archive servers can be brought down with no loss of data or functionality. As many U-Series Appliances may be added as required and pointed at the availability group.

Note: *Only one admin (manager) service is supported at any one time but this may be configured to failover to a secondary U-Series Appliance.*

Microsoft SQL Always On Availability Groups may consist of a primary replica, and up to 8 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 U-Series Appliance available (https://aws.amazon.com/marketplace/seller-profile?id=edb65982-bb22-445e-854b-c1156a5026d9), and an Azure U-Series Appliance.

DR Primary Sites Scenario 1 - Loss of a Database Server

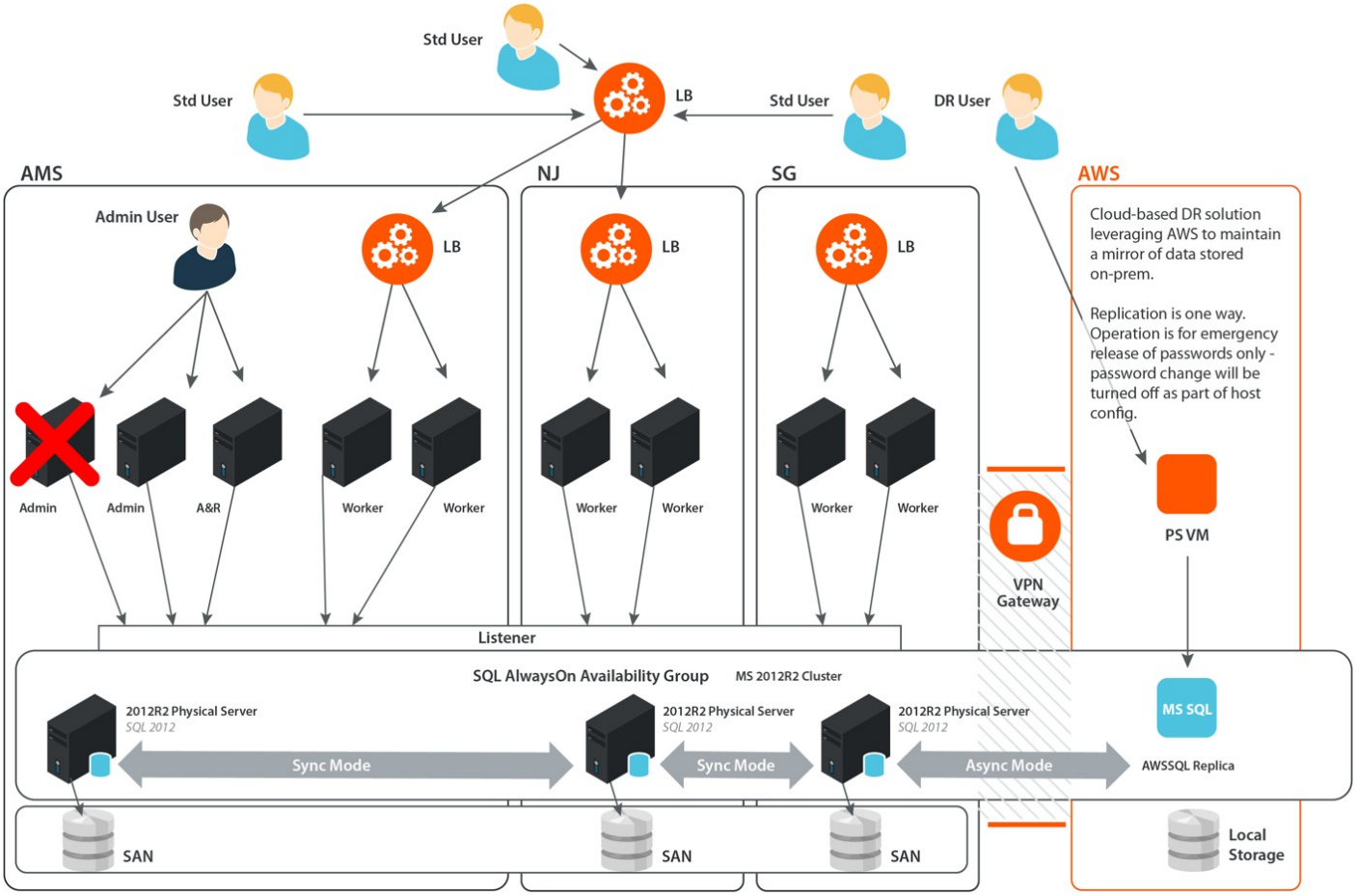


For an environment using SQL Always On, a minimum of two synchronous-commit replicas is assumed. In the event that the replica holding the primary role fails, the secondary replica may be set to automatically (or manually) become the new primary. In general use, secondary replicas are used for redundancy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

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

> *For a more comprehensive set of failover scenarios please see Always On availability groups: a high-availability and disaster-recovery solution at https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server.*

DR Primary Sites Scenario 2 - Loss of the Admin U-Series Appliance



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

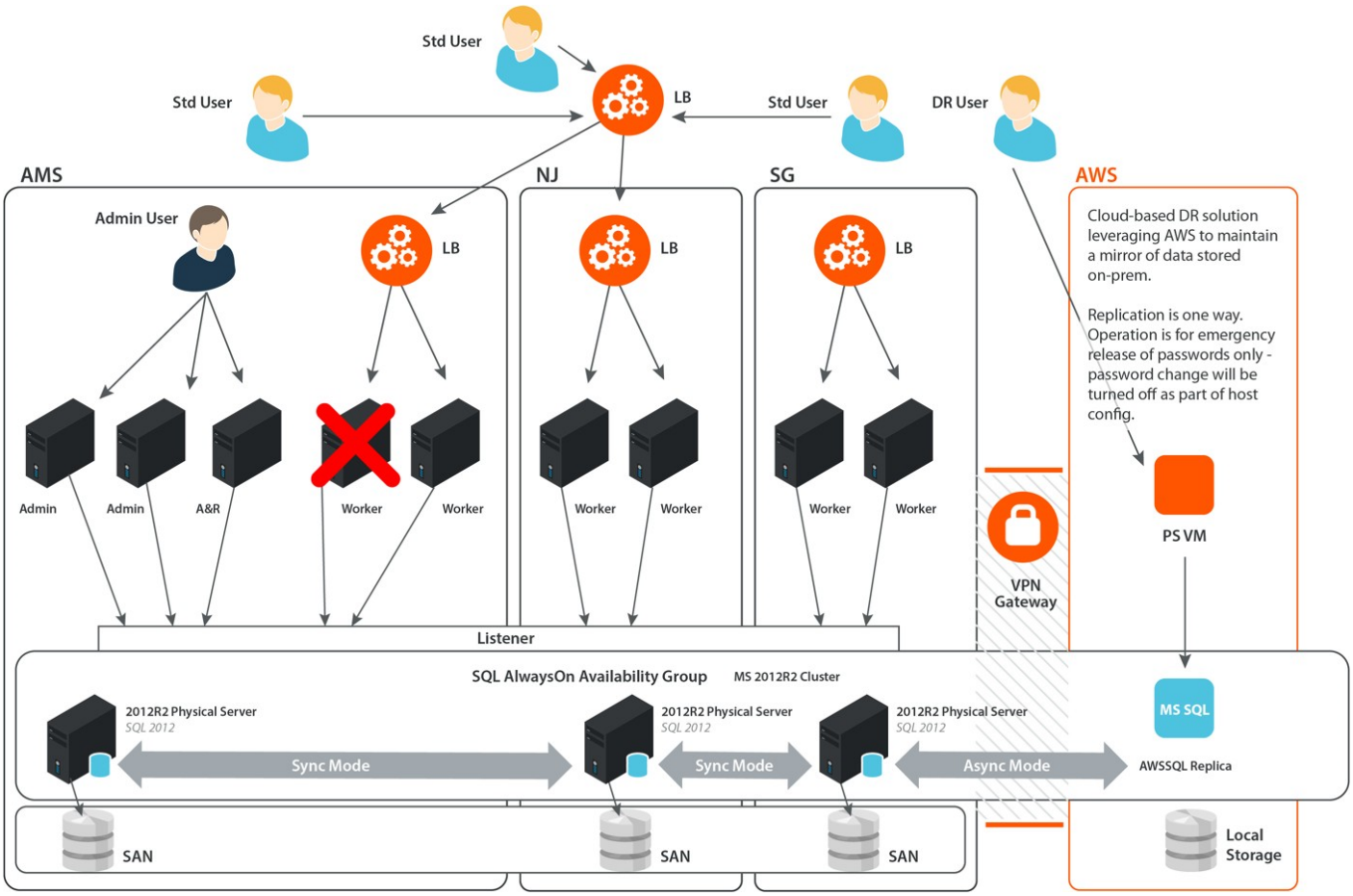
There can only be one node running the BeyondInsight interface at one time due to potential contention between more than one Manager Service.

U-Series Appliances have multiple roles that may be configured at any time. If a U-Series Appliance running the Admin role fails, or is brought offline, an alternate U-Series Appliance may be configured with the Admin role. We recommend, 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 U-Series Appliance, 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 are affected if no Admin node is available; however, any scheduled password changes that have already been added to the central database queue continue to be serviced by the worker nodes, and any end user-based request operations are unaffected.

DR Primary Sites Scenario 3 – Loss of a Worker U-Series Appliance



U-Series 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**: Searching and replaying user sessions

In the event that a U-Series Appliance fails or becomes unavailable for any reason (network outage, etc.), the user may be automatically redirected via load balancer to an alternate U-Series Appliance 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 is resubmitted on next job execution.

Password Portal

Users that are logged in when loss of service occurs are redirected via load balancer to an alternate U-Series Appliance. 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 is connecting to the VIP/listener of the load balancer, the user should be redirected to the same session they were in when the failover event happened.

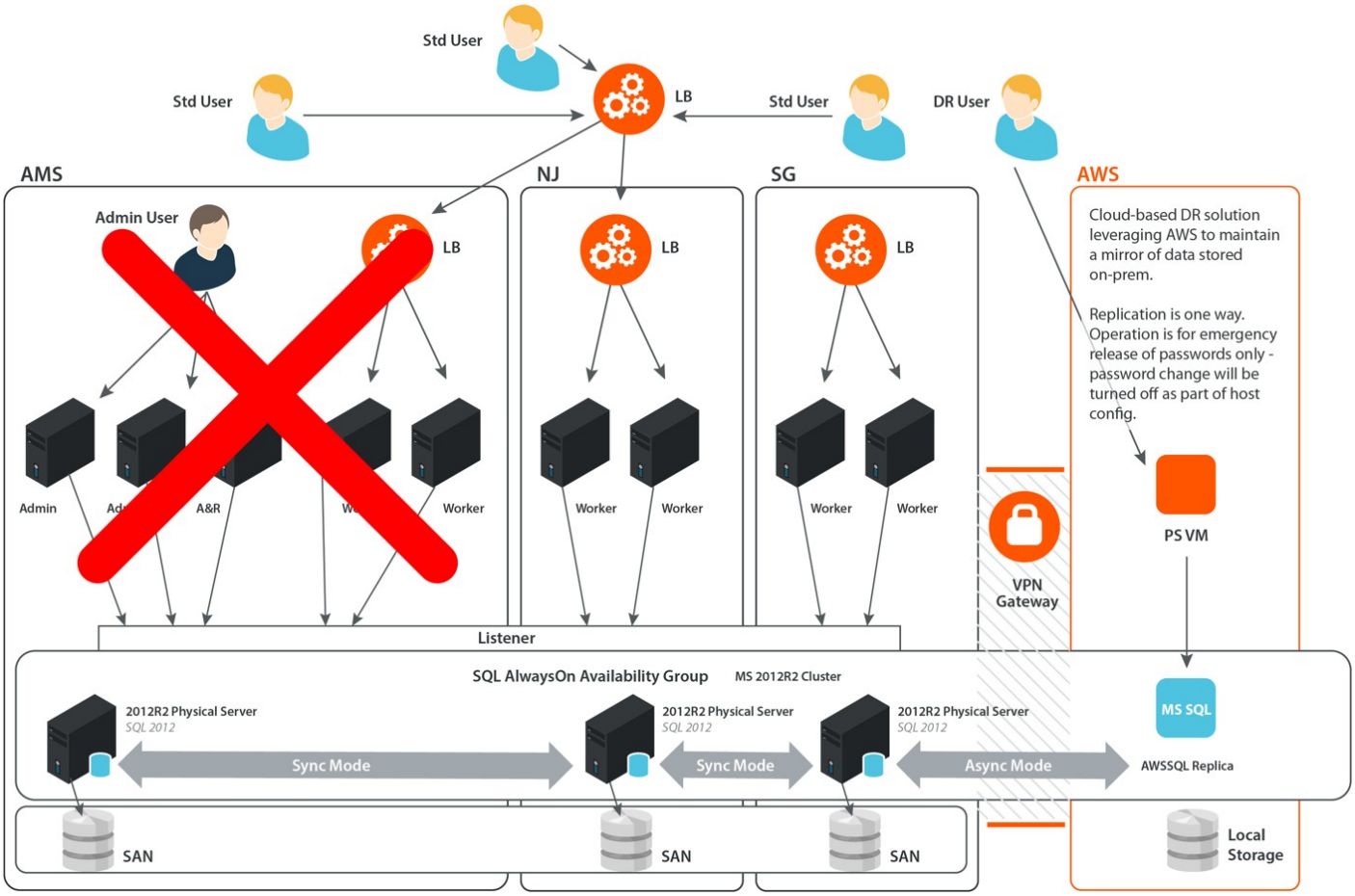
Session Recording (proxy)

Any sessions that are in process are halted. When the user is redirected to an alternate proxy, a new RDP/SSH/Application session is established with their target host. If the failover event is catastrophic, and the original U-Series Appliance is unrecoverable, any session video recording files that were in process when the event occurred are lost. To safeguard historical recordings, we recommend you implement an archive server *zero-retention* strategy as indicated 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 continues to service password requests / messages from the central database queue. **Queue Agents** may be configured such that they service only requests for specific groups of accounts. In this manner, loss of an agent in New Jersey results in the alternate New Jersey agent taking over the request processing.

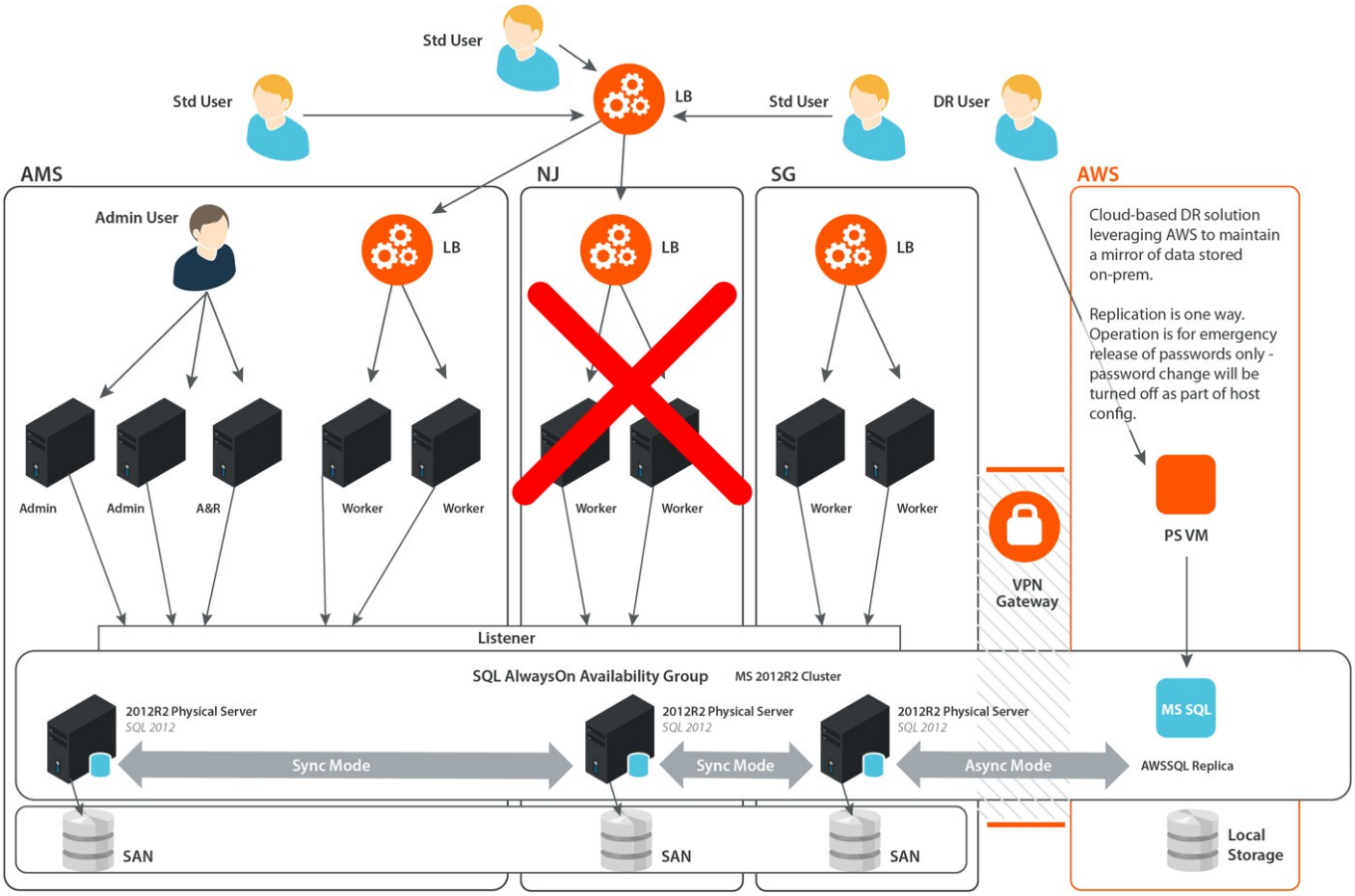
DR Primary Sites Scenario 4 – Loss of the Primary Site



If the primary site containing read/write database replicas were to go offline, the following actions should be observed or 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 U-Series 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 U-Series Appliance, or the reporting database restored to a backup U-Series Appliance.
4. Users should automatically be redirected to an alternate U-Series Appliance portal via load balancers.

DR Primary Sites Scenario 5 – Loss of a Secondary Site

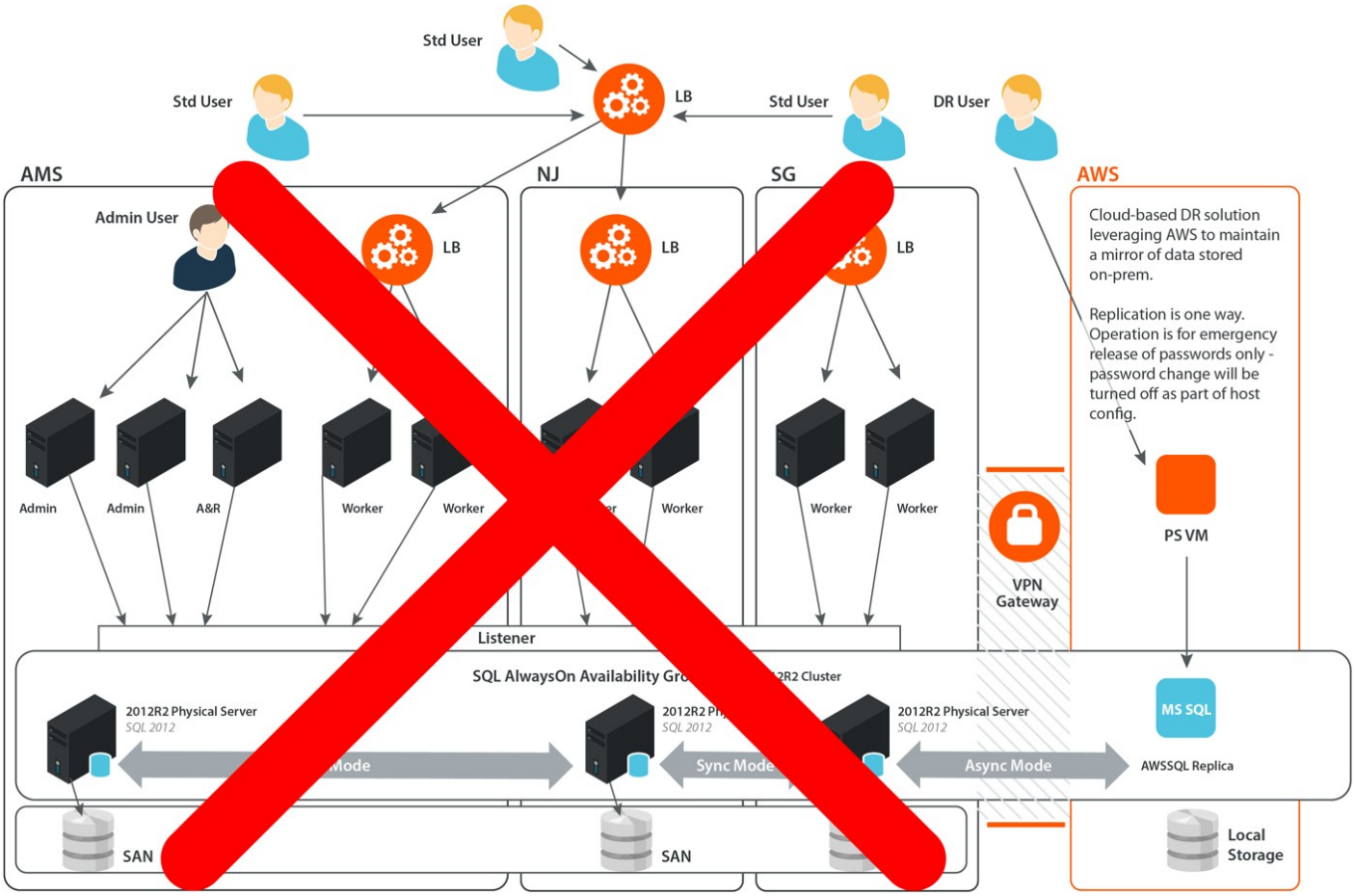


In the event that a secondary site were to go offline, users would be automatically redirected by the load balancers to either one of the alternate sites in operation.

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 U-Series Appliances in the site that suffered an outage, such that those password change events may be serviced by U-Series Appliances from the alternate sites.

DR Primary Sites Scenario 6 – Loss of Access to All On-Prem Infrastructure

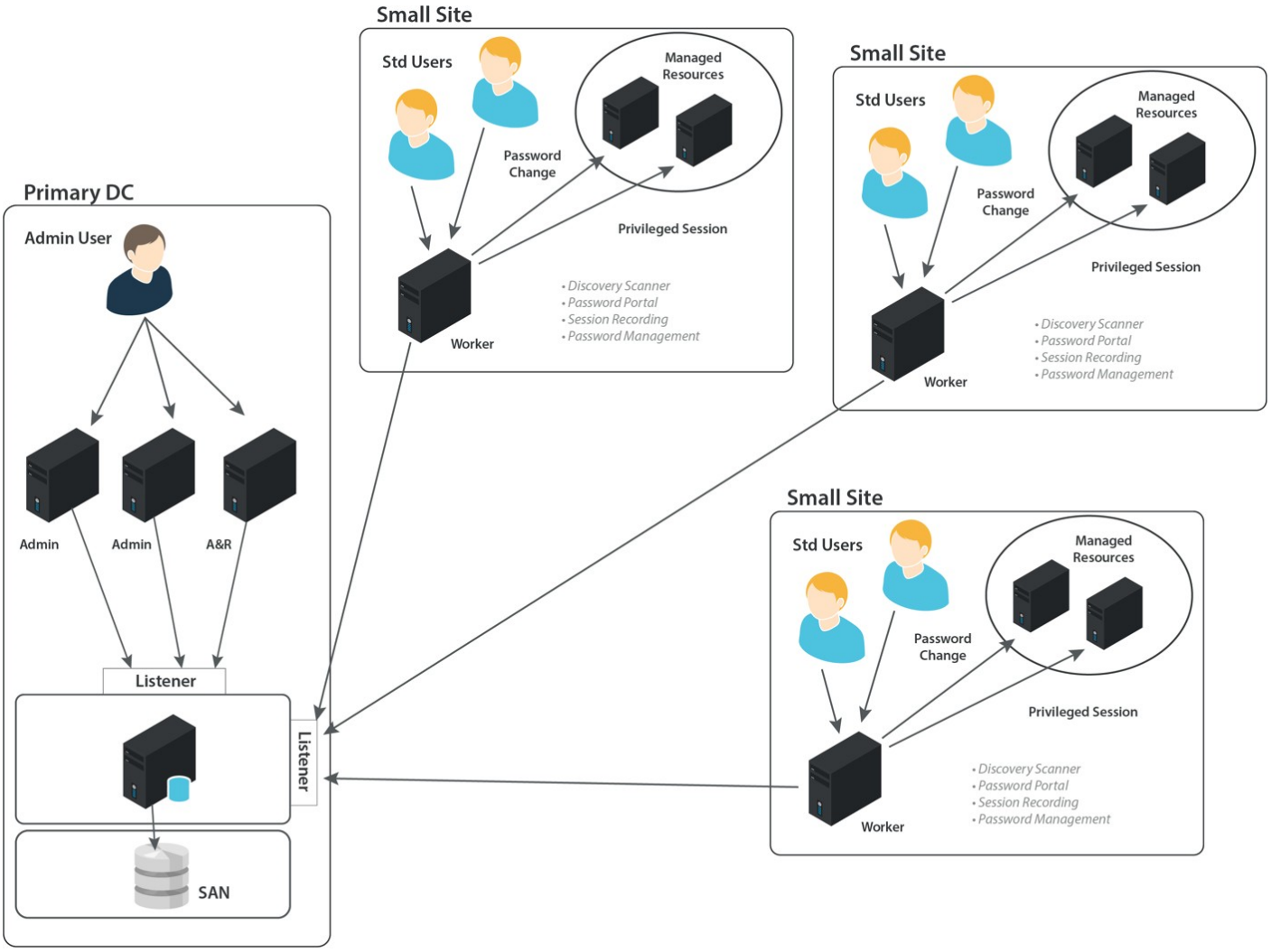


If access to all on premise systems were affected, the following methodologies should be taken into consideration:

- **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.
- **Longer-term outage**: database restoration and key U-Series Appliance restoration into tertiary data centers. Note that U-Series Appliance 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 whether or not you care about password rotation in a DR scenario, or if you can wait until you have recovered.

> ***Note:*** *This document is not intended to be a detailed blueprint of data center DR best practices but instead guidelines for cases where Endpoint Privilege Management 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



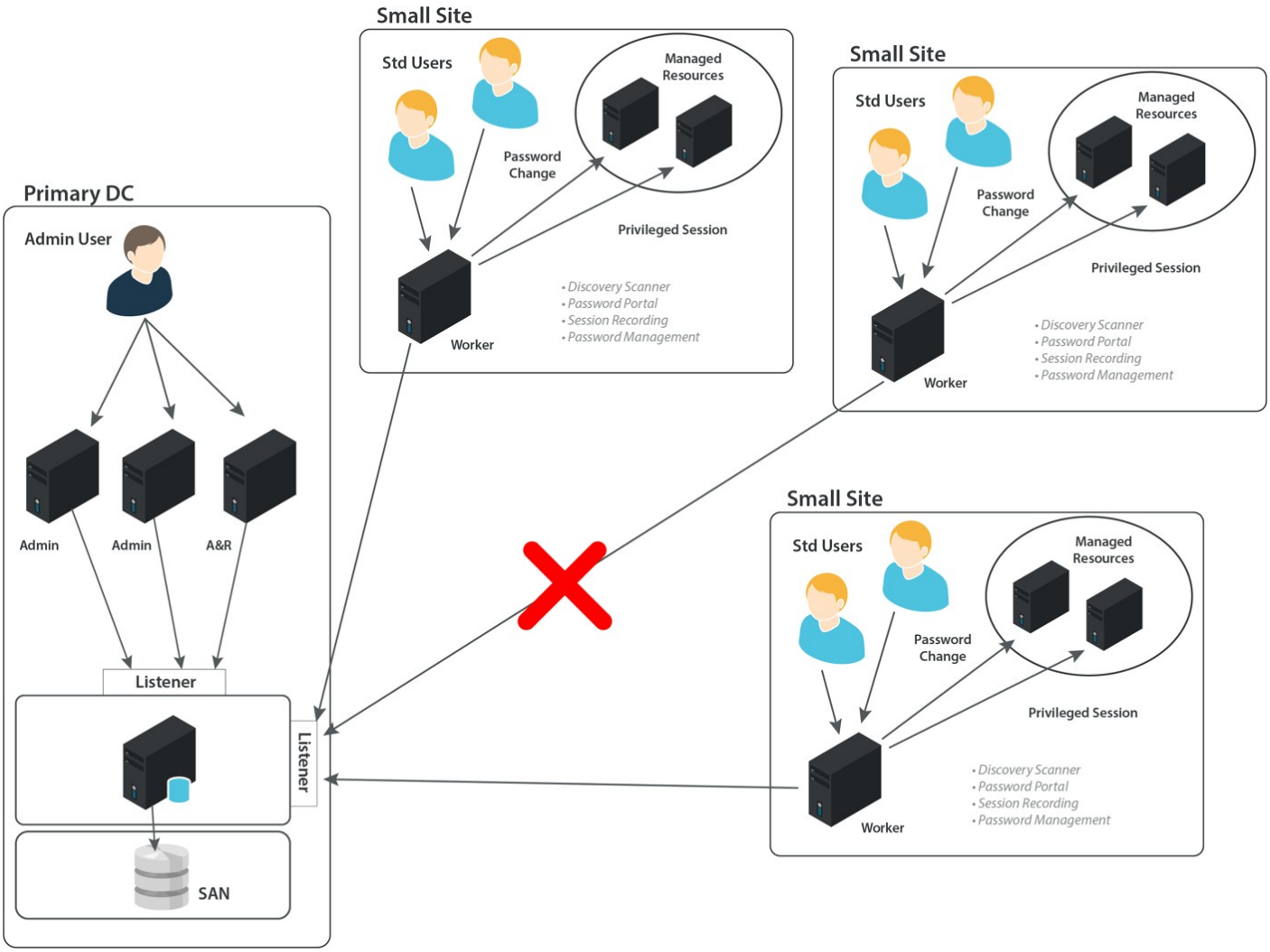
In this scenario, the node is configured with a workgroup name specific to the site; all managed accounts on the site are configured with the same workgroup. In this manner each worker node would be responsible for changing just the passwords for the site it is located in.

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**: Searching and replaying user sessions

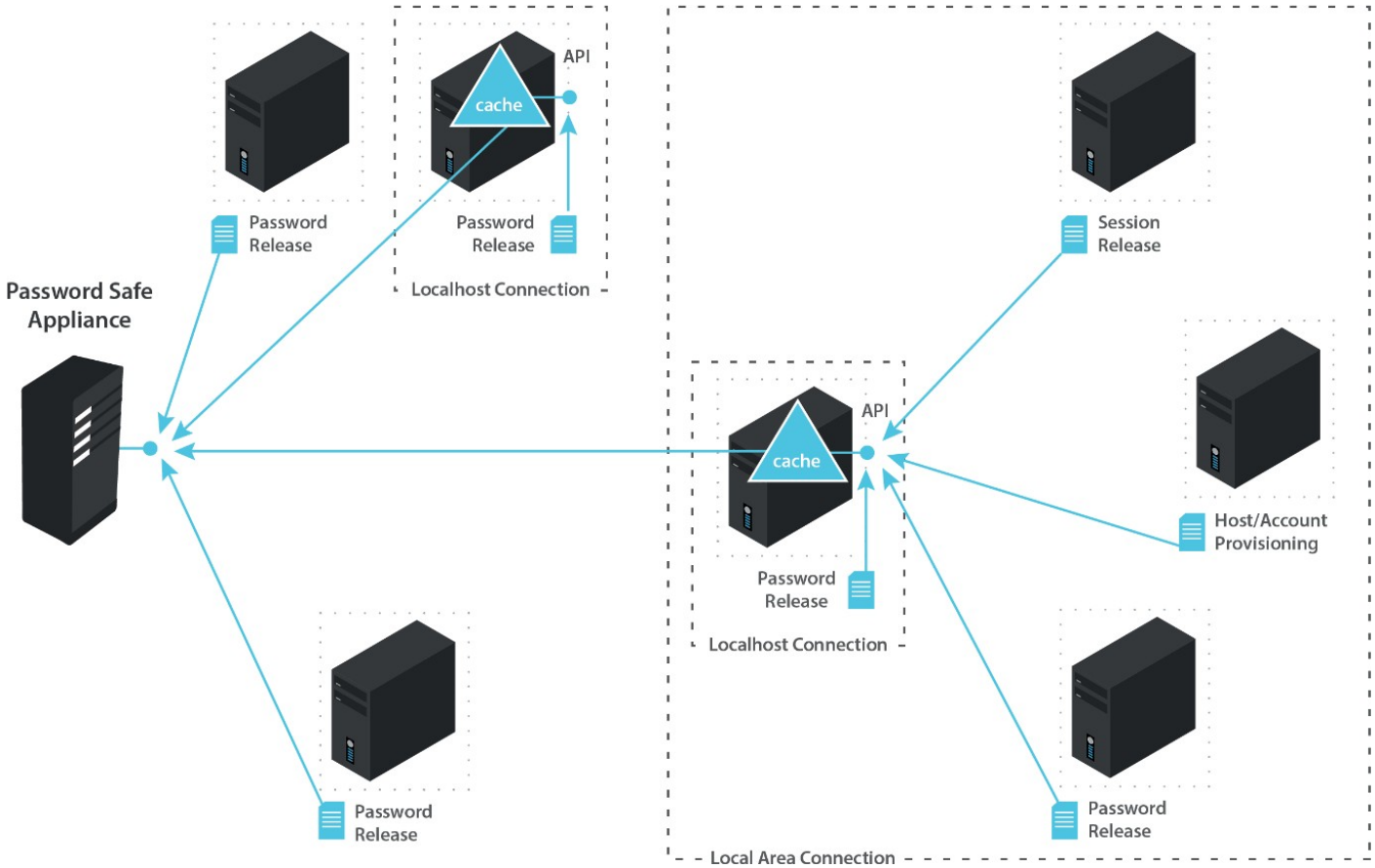
Sessions are proxied via the local worker node; recorded keystrokes (if applicable) are stored in the central database; recorded session files may be stored locally on the node according to retention rules or transferred immediately to central archive storage locations.

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



In the current architecture, any separation from the central database prevents users from logging on to the worker node.

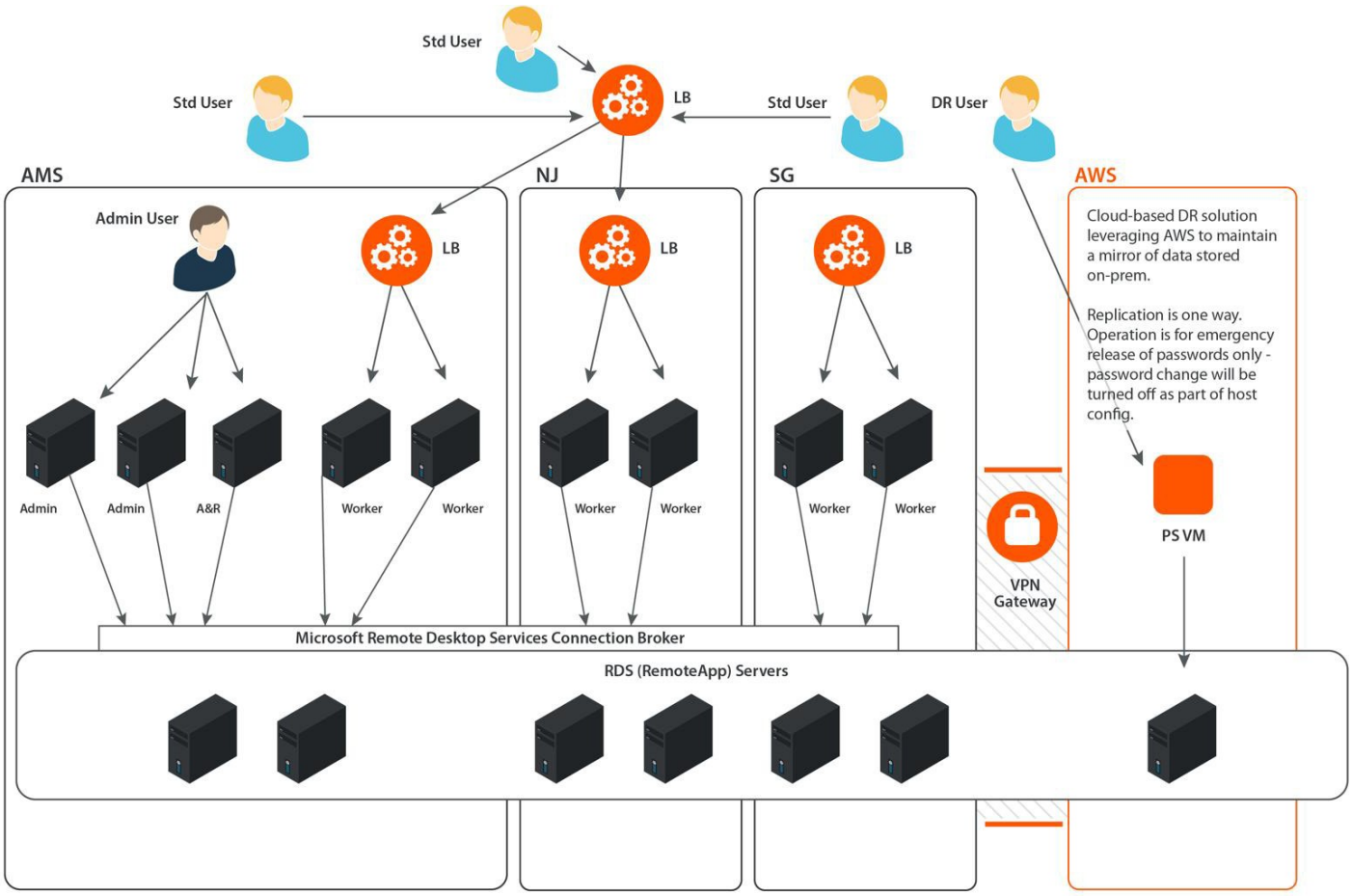
As a mitigating step, it is possible to install an unlimited number of Password Caches in the Password Safe environment to persistently store credentials in the event of an outage.



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.

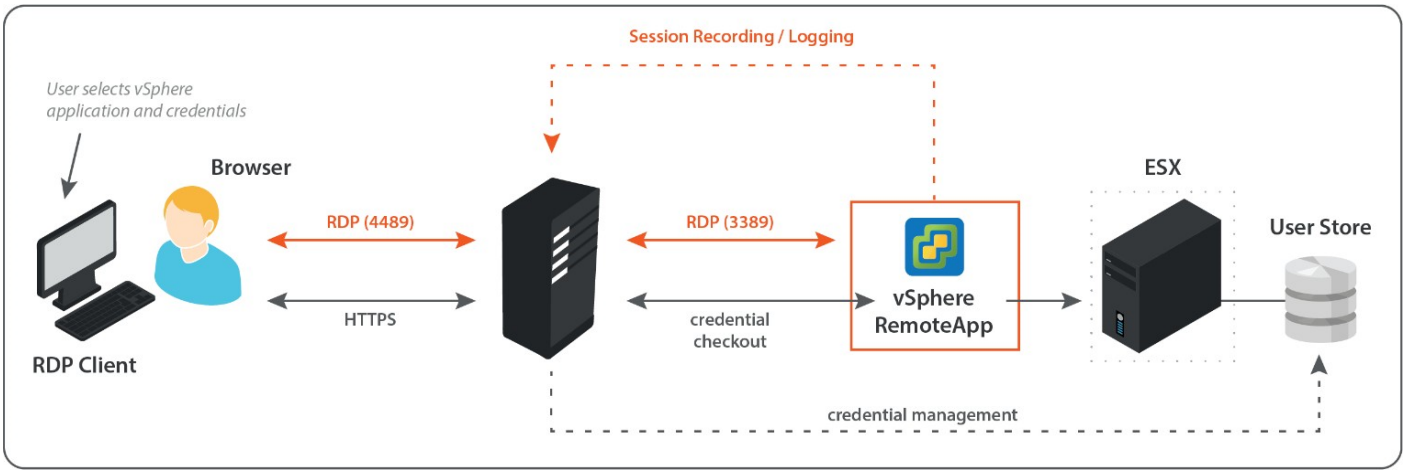
DR RemoteApps Deployment

Example RemoteApp Architecture



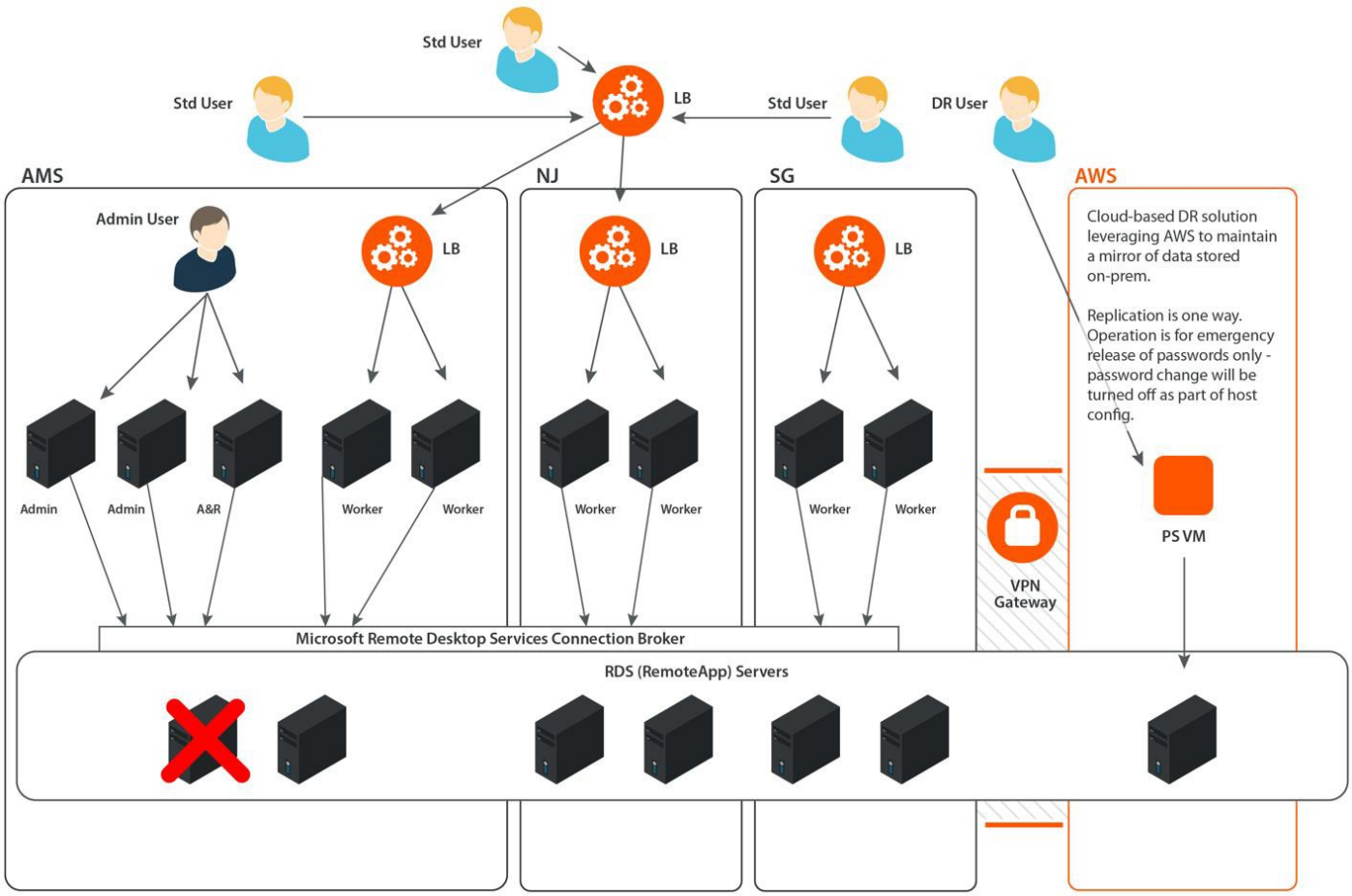
Proxy Failure Scenarios

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.



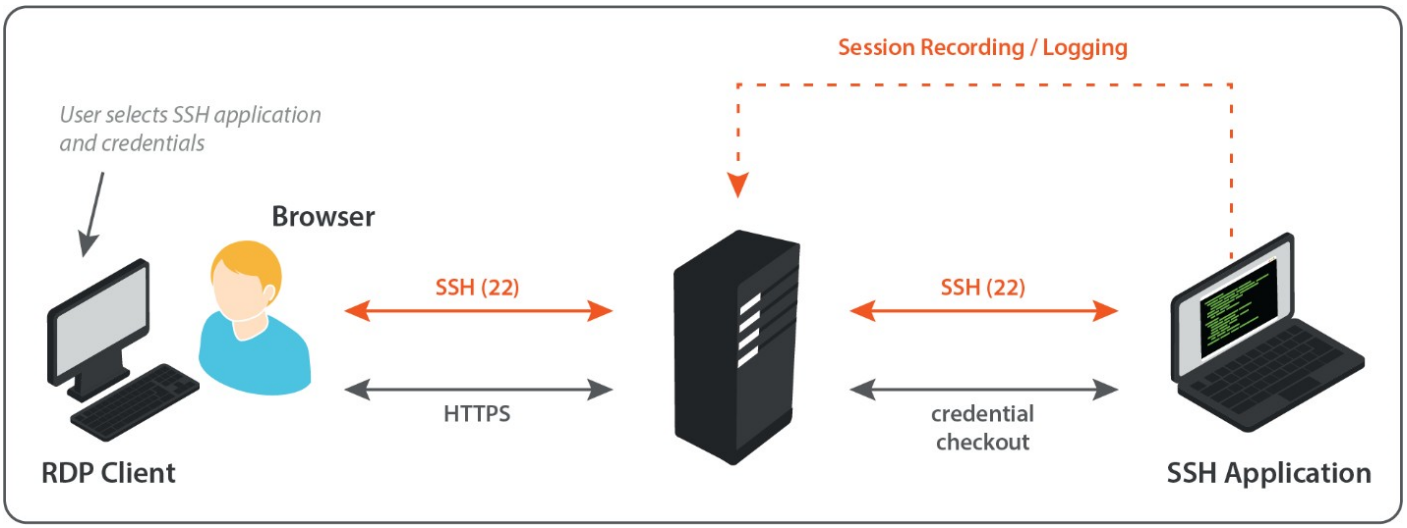
In the event of U-Series Appliance/proxy failure, the user is redirected to an alternate worker node where they can establish a new connection using the same checked out session.

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 U-Series Appliance.



In the event of U-Series Appliance/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.

Default Ports

System Discovery

Functionality	Service	Ports	Requirements/Notes
User Enumeration	nb-ssn | ms-ds	TCP 139 / 445[1]	
Hardware Enumeration	nb-ssn | ms-ds	TCP 139 / 445[2]	WMI Service running on target
Software Enumeration	nb-ssn | ms-ds	TCP 139 / 445[3]	Remote Registry service running on target
Local Services	ms-ds	TCP 445	

Desktop Connectivity

Functionality	Service	Ports
User Interface	https	TCP 443
Remote Desktop	rdp	TCP 4489
SSH	ssh	TCP 4422

Session Management

Functionality	Service	Ports
Remote Desktop	rdp	TCP 3389
SSH	ssh	TCP 22

Network Devices

Functionality	Service	Ports
Checkpoint	ssh	TCP 22
Cisco	ssh	TCP 22
Dell iDRAC	ssh	TCP 22
F5 BIG IP	ssh	TCP 22
HP Comware	ssh	TCP 22
HP iLO	ssh	TCP 22
Juniper	ssh	TCP 22
Palo Alto	ssh	TCP 22

[1] 445 preferred.
[2] 445 preferred.
[3] 445 preferred.

Fortinet	ssh	TCP 22
SonicWall	ssh	TCP 22

Operating Systems

Functionality	Service	Ports	Requirements/Notes
AIX	ssh	TCP 22	
HP-UX	ssh	TCP 22	
IBMi (AS400)	telnet	TCP 22	
Linux	ssh	TCP 22	
MAC OSX	ssh	TCP 22	
Solaris	ssh	TCP 22	
Windows Desktop	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389	ms-ds (TCP 445) is used as a fallback
Windows Server	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389	ms-ds (TCP 445) is used as a fallback
Windows Update/Restart Service	wmi	TCP 135	WMI Service running on target

Directories

Functionality	Service	Ports	Requirements/Notes
Active Directory	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389	ms-ds (TCP 445) is used as a fallback
RACF	ssh	TCP 22	
LDAP/S	ldap ldaps	TCP / UDP 389 TCP 636 / UDP 389 TCP 88 (Kerberos) TCP 80 (CRL Validation) TCP 135 (RPC) TCP 389 (LDAP) TCP 445 (CIFS) TCP 464 (Directories) TCP 636 (LDAPS) TCP 3268 (Global Catalog) TCP 3269 (Global Catalog LDAPS)	

Databases

Functionality	Service	Ports
Oracle	oracle-listener	TCP 1521

MS SQL Server	netlib	TCP 1433
Sybase ASE		TCP 5000
MySQL		TCP 3306
Teradata		TCP 1025

Applications

Functionality	Ports
VMware vSphere API	API
VMware vSphere SSH	TCP 22
SAP	API

U-Series Appliance

Functionality	Service	Ports
Mail Server Integration	smtp	TCP 25
AD Integration	ldap ldaps	TCP / UDP 389 TCP 636 / UDP 389
Backup	smb	TCP 445
Time Protocol	ntp	UDP 123
HA Replication (pair)	sql-mirroring | https	TCP 5022 / 443