BeyondInsight and Password Safe Deployment Whitepaper

Powered By PowerBroker

TC:5/14/2019

Table of Contents

BeyondInsight and Password Safe Deployment Whitepaper

Password Safe is your privileged access management solution to ensure your resources are protected from insider threats.

Using Password Safe, you can restrict access to critical systems, including assets and applications, keeping them safe from potential inside threat risks.

Password Safe is supported on a UVM (Unified Vulnerability Management) hardened appliance that creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system.

Active-Active Deployment Model for Password Safe

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).

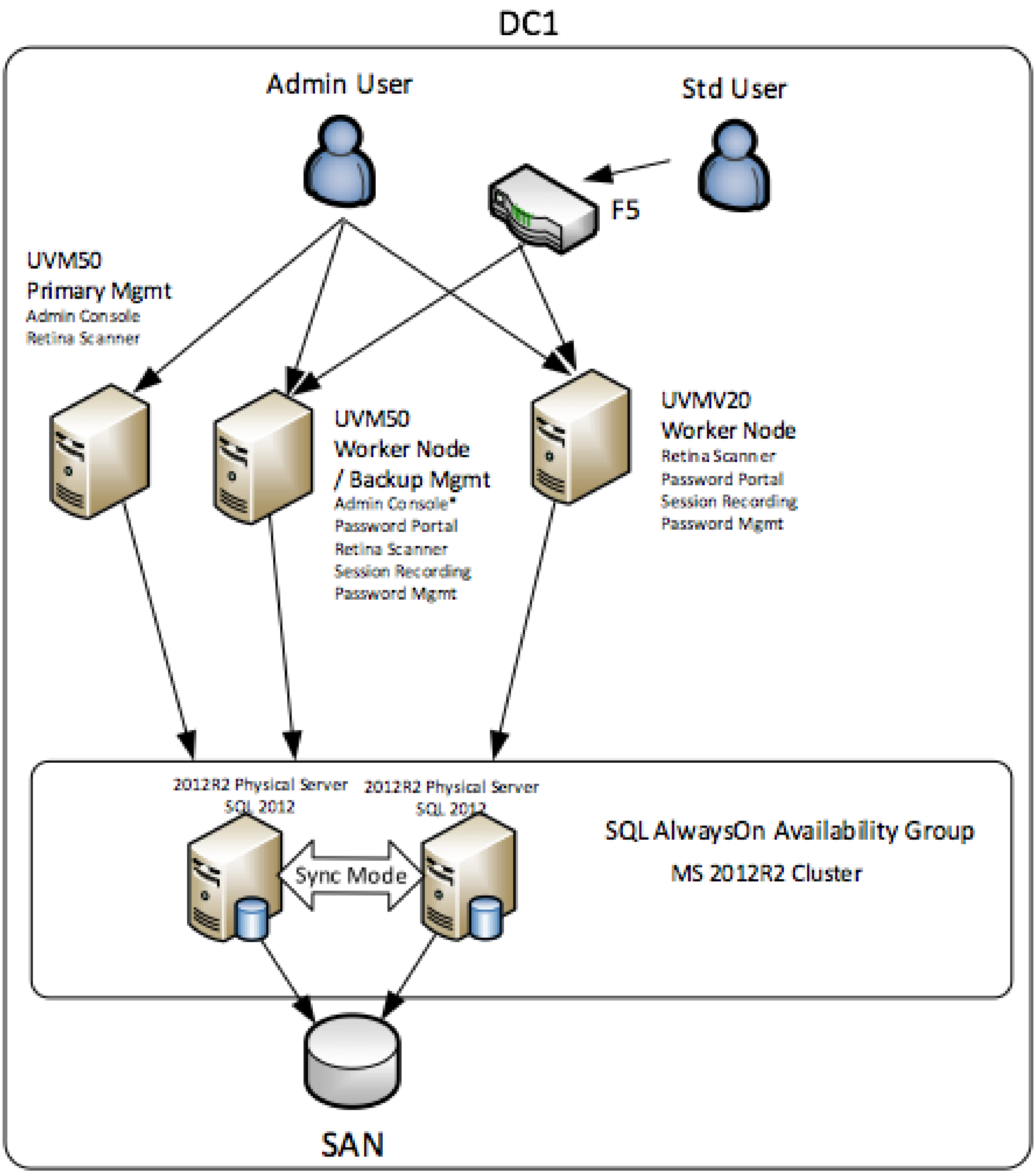
As many appliances as required can be configured to connect to the database. In this case, all appliances can be used at once, and are fully redundant; if one goes down, you switch to an alternative. AlwaysOn Availability Groups may be configured with a mix of synchronous commit and asynchronous commit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

The following deployment sections are provided as a high-level overview scenario.

Single Site Deployment

A single site can 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 can be made directly, or via a load balancer. Both appliances can 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 or retention.

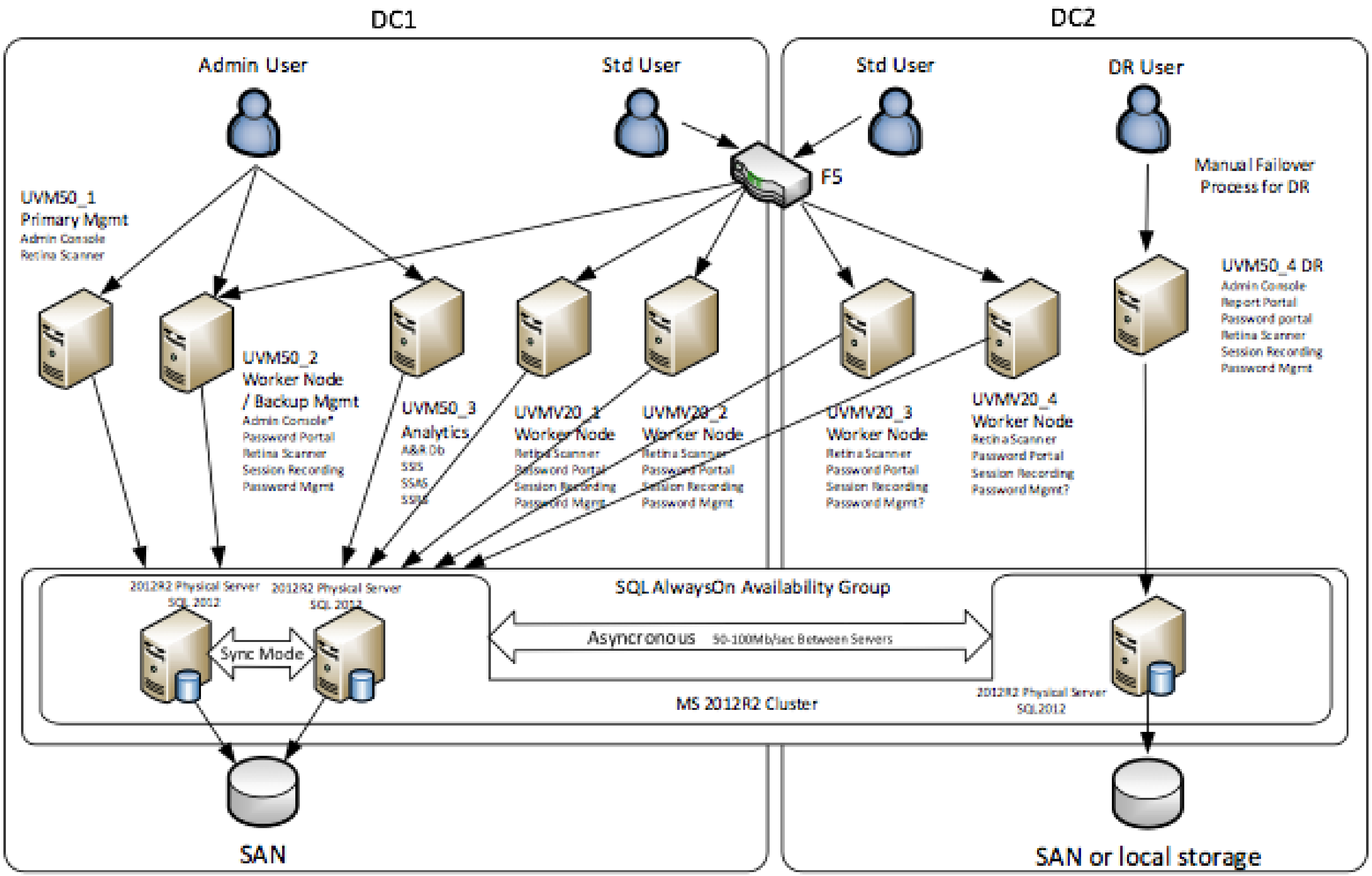

DC1
Admin User
Std User
F5
UVM50
Primary Mgmt
Admin Console
Retina Scanner
UVM50
Worker Node
/ Backup Mgmt
Admin Console*
Password Portal
Retina Scanner
Session Recording
Password Mgmt
UVMV20
Worker Node
Retina Scanner
Password Portal
Session Recording
Password Mgmt
2012R2 Physical Server
SQL 2012
2012R2 Physical Server
SQL 2012
Sync Mode
SQL AlwaysOn Availability Group
MS 2012R2 Cluster
SAN

Multi-Site Deployment

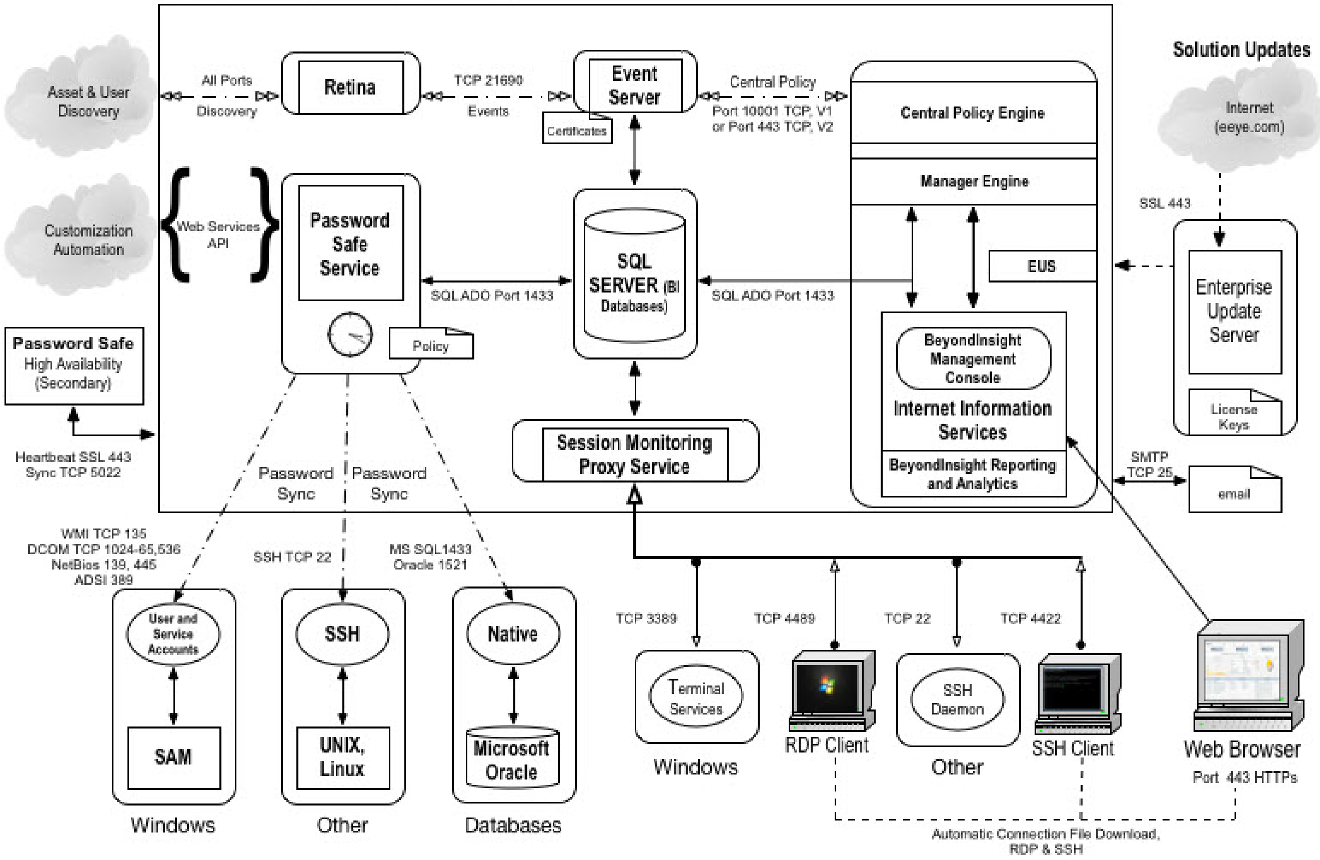
In this example, multiple data centers are connected to an AlwaysOn Availability Group. It can be seen that many more appliances can be added, each with varying roles, such as: Scanners; Event Servers, Password Portals, Session Managers, and Password Management.

Behind load balancers, 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 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:*** *Only one manager service is supported but this may be configured to fail over to a secondary appliance. Also note that 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.*



BeyondInsight & Password Safe Architecture



Password Safe Scalability

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

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