



Software Robots - the Virtual Workforce

Virtualization

REFERENCE GUIDE

Major Version: 6
Document Revision: 1.0

For more information please contact:

info@blueprism.com | UK: +44 (0) 870 879 3000 | US: +1 888 757 7476

www.blueprism.com

Contents

| | |
|---|----|
| 1. Introduction..... | 3 |
| 2. Defining an Appropriate Virtualization Strategy..... | 4 |
| 3. Selecting the Virtualization Technology..... | 4 |
| 4. Designing the Virtual Platform..... | 13 |
| Appendix A – Known Issues | 15 |

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third party without the written consent of an authorised Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

© Blue Prism Limited, 2001 – 2017

®Blue Prism is a registered trademark of Blue Prism Limited

All trademarks are hereby acknowledged and are used to the benefit of their respective owners.
Blue Prism is not responsible for the content of external websites referenced by this document.

Blue Prism Limited, Centrix House, Crow Lane East, Newton-le-Willows, WA12 9UY, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

1. Introduction

1.1. Intended audience

This reference guide is intended for use by Enterprise Architects, who are involved in designing a Virtualized implementation of the Blue Prism product.

1.2. About this document

The document explains the key factors that should be considered when designing or deploying a Blue Prism environment in a Virtualized environment.

It is recommended that readers should be familiar with the various components that feature within a Blue Prism environment, as described within the Infrastructure Reference Guide. A reasonable level of knowledge and experience in Virtualization topics is assumed. Blue Prism does not recommend or endorse a particular Virtualization technology, therefore this document covers topics in a product agnostic way, wherever possible, however some specific products may be used as examples.

1.3. Information

Within this document there may be external references to data sheets and user guides that focus on specific topics – such references will be presented [underlined and colored blue](#) for ease of identification.

2. Defining an Appropriate Virtualization Strategy

2.1. Overview

Blue Prism is an Enterprise solution and will generally be deployed within a Data Center. In most cases, this will involve deployment on a Virtualized platform. It is essential that an Architect with knowledge and experience in Virtualization is involved in the design of the final solution.

At a high level, defining the Virtualization strategy for the Blue Prism RPA solution will involve the following 2 key stages:

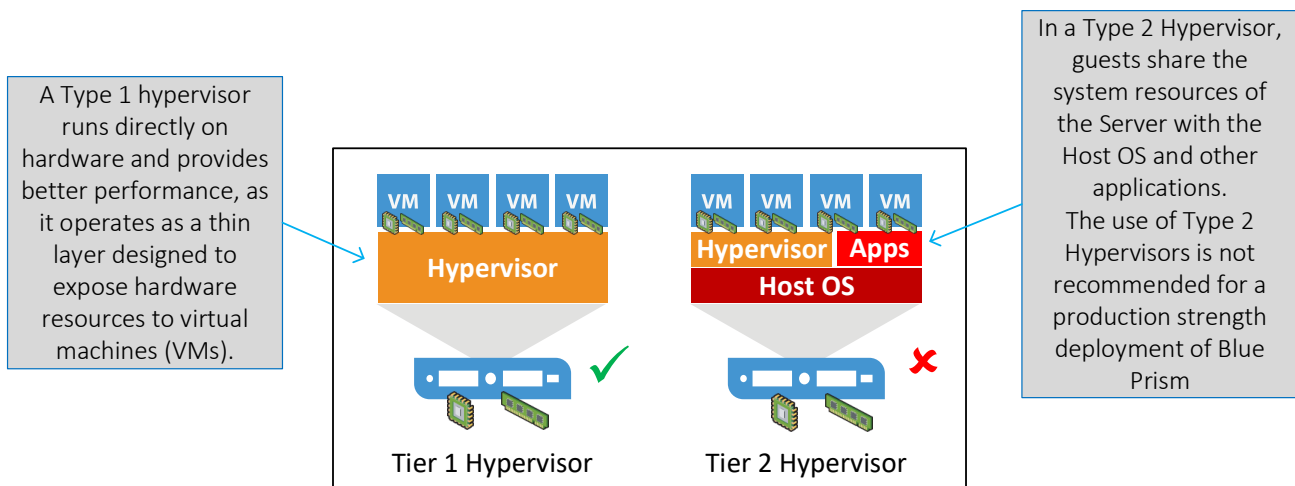
- Defining the overall Virtualization Strategy - considering all functional and non-functional requirements for the environment. These are likely to include consideration of one or more of the following:
 - Existing Data Center and Virtualization Strategies and Components
 - Desktop Virtualization Strategies and Software
 - Security
 - Support
 - Performance
 - Availability
- Designing the environment – including the specification of the physical hosts, defining a Virtualization strategy for each core component of the application and defining any interaction with peripheral components or software – such as Active Directory, monitoring and backup.

3. Selecting the Virtualization Technology

Taking into account the Functional and non-Functional requirements for the solution, the first step in defining the strategy for Blue Prism is to select the Virtualization Technology that will be used. The following sections provide some high level guidance in selecting the appropriate options.

3.1. Selecting an Appropriate Hypervisor

There are 2 types of Hypervisor. These are commonly referred to as “Type 1” and “Type 2”. These 2 types of Hypervisor are depicted in the diagram below:



Type 1 Hypervisors include:

- VMware vSphere
- Citrix XenServer
- Microsoft Hyper-V
- KVM

Type 2 Hypervisors include:

- VMware Fusion / Workstation / Player
- Oracle VirtualBox

Additional considerations may also include:

- Ensuring that the Hypervisor provides support for the operating system(s) that will be deployed onto the virtual instances - For example ESX 3.5 (prior to update 5 (U5)) is incompatible with Windows 7.
- Security and Remote Console Access - Most Hypervisors will provide console level access to the VMs, which should be secured to prevent unauthorised access to view or influence the execution of automated transactions. This console level access may also be considered as a secure method for non intrusive remoting of Robots, if required. Further information on Remoting Technology considerations is contained within the following document: [Blue Prism Data Sheet – Remote Access Tools](#)
- The existing Data-Center or Enterprise Virtualization Strategy and Technology - Alignment to an existing Virtualization strategy or platform will provide obvious support and maintenance benefits, but consideration should be given to whether this will adequately support the requirements of the Blue Prism environment.
- Existing Desktop Virtualization strategies - The use of Desktop Virtualization technology is a significant topic in its own right and is covered below in section 3.3.

3.2. Blue Prism Component Virtualization Quick Reference

The following table may be used as a reference guide to aid in selecting the appropriate Virtualization strategy for each component. Refer to the detailed sections for additional guidance.

| Blue Prism Component | Suitability for Virtualization | Key Design Considerations |
|----------------------|--------------------------------|--|
| Database | ! | <ul style="list-style-type: none"> • Production instances will normally be implemented on separate physical hardware. • Consider all Vendor documented best practices • Refer to section 4.4.1 – Database Server, for further guidance. |
| Application Server | ✓ | <ul style="list-style-type: none"> • Consider using HA techniques such as VMware HA and DRS rules to ensure adequate distribution between hosts. |

| | | |
|----------------------------|---|---|
| Runtime Resources | ✓ | <ul style="list-style-type: none"> • Should be virtualized to ensure security, availability and consistency • Consider using HA techniques such as VMware HA and DRS rules to ensure adequate distribution between hosts. • Right sizing will depend on an understanding of the entire platform (OS + Blue Prism requirements + Automated applications). • Refer to section 4.4.2 – Runtime Resources, for further guidance |
| Interactive Client Systems | ✓ | <ul style="list-style-type: none"> • Development Operating environment should be identical to the Runtime Resources • Consider using HA techniques such as VMware HA and DRS rules to ensure adequate distribution between hosts. • Right sizing will depend on an understanding of the entire platform (OS + Blue Prism requirements + Automated applications). • Refer to section 4.4.3 – Interactive Clients, for further guidance |

3.2.1. Database Server

As a general rule, Blue Prism would recommend implementing the Database server onto a separate physical environment, as this will offer the best performance in large scale environments. It is recognised however, that the considerations involved in determining suitability of SQL Server for a virtual platform are far reaching and vary greatly, depending on overall strategy and design. These requirements span multiple dimensions, such as availability, performance, scalability, growth and headroom, patching, and backups.

If there is a desire to virtualize the database component, it is essential to assure appropriate levels of physical hardware resource are provided, and that any vendor specific guidelines from both Microsoft and the Virtualization technology provider (e.g. Citrix, Microsoft, VMware etc.) are adhered to. SQL Server databases are extremely sensitive to the performance of the underlying hardware and therefore if the virtualized resources are not adequately sized, the performance of the Blue Prism environment will be affected. Consider also if the underlying resources are shared by additional components, as this may result in contention which will further impact performance.

External Guides:

The following vendor provided external guidance may be used in order to properly design a Virtualized Microsoft SQL Server environment. Note that these guides are not endorsed or actively reviewed by Blue Prism.

VMware vSphere: [Architecting Microsoft SQL Server on VMware Vsphere](#)

Microsoft: [Best Practices for Virtualizing and Managing SQL Server 2012](#)

3.2.2. Runtime Resources (Robots)

Runtime Resources are commonly Virtualized components within the Data Center. This is the recommended deployment approach, for the following reasons:

- Consistency – The use of a common build standard for the Virtualized robots ensures a consistent platform, which minimises any risk of processes being impacted by environmental differences when distributing workload between the robots.
- Security – The use of a Hypervisor enables an additional layer of security across the Virtual resources. Hypervisor level security can be used to restrict the users who may access the console of the runtimes.
- Control – By virtualizing the Runtimes, the IT department can carefully manage and monitor the performance of the Runtimes and easily scale up or out the Virtualized devices as required to support the managed processes.
- Availability – The use of Virtualization enables additional options for High Availability and Disaster Recovery scenarios, using techniques such as VMotion, DRS rules and VMware HA.

Design Considerations:

When designing the Virtualized platform for the Runtime Resources, the following key points should be considered:

- OS Build – The base image for the Runtime Resources should ideally be as close as possible to the operating environment used by the Human resources performing the tasks today. It is essential that it is identical to the Interactive Client systems used for Development, in order to ensure a common operating platform throughout the development and release cycle. Using the standard desktop image for a user as a basis for the Runtime is often not practical (due to additional software that is included, but not appropriate for the unattended Robot environment, for example). It may be necessary to create a separate build standard. The base image should also include the software required for Blue Prism itself, unless this will be installed or applied separately.
- System Resources – The Infrastructure Reference guide contains recommendations for the minimum specifications required for a Runtime Resource. This recommendation is based on the minimum required to execute the Blue Prism software. In most cases, it is also necessary to consider the resource requirements for the applications being instrumented by the Software. A good rule of thumb is to take the standard specification of the device being used by human operators as a starting point, if an individual assessment of the application requirements is not feasible. Consider creating tiered specification standards for the VMs, to allow for some flexibility and standardisation in managing the environment.

3.2.3. Interactive Client Systems

Where dedicated Interactive Client Systems are deployed (ie, when the Interactive Client software is not installed on an existing user's desktop), these components should be virtualized, for the following reasons:

- Consistency – The use of a common build standard between the Interactive Development clients and Runtime Resources reduces the potential for issues when moving workload between Development and Production.
- Control – By virtualizing the Interactive Client systems, the IT department can carefully manage and monitor the performance and easily scale up or out the devices, as required to support a specific Process.

- Network – By locating the Interactive Client systems topologically close in the network to the Runtime Resources, the risk of experiencing inconsistent performance or connectivity issues when moving processes into production are minimised. This model is also supportive of Geographically separated Blue Prism Controllers.

Design Considerations

The design considerations are similar to those specified for the Runtime Resources – consistency between the Interactive Client systems and Runtime Resources is key.

3.3. Desktop Virtualization

The subject of Desktop Virtualization is broad and often encompasses several technologies, which are often overlapping and sometimes conflicting. The core topics are explored in this section.

3.3.1. Desktop Virtualization Technology Terminology and Reference

The following section is intended to provide a high-level explanation of each topic and any key considerations or terminology, in order that the implications of each may be explored further within the subsequent sections.

Virtual Desktop Infrastructure (VDI) / Hosted Virtual Desktop (HVD)

Generally, refers to Technology where the Desktop Operating System is isolated within a Virtual Machine on a separate Physical Server, usually via a Type 1 Hypervisor. These VMs will have dedicated system resources.

Hosted Shared Desktop (HSD), or Presentation Virtualization

Generally, refers to Technology where a user is presented with a desktop and / or “published” applications, from a multi-tenant presentation server. The key point to note here is that resources are shared between all users and sessions can only be persistent when a user is connected. The other implication is that the application is not running locally on the machine, which would limit the possible automation techniques (Surface Automation would need to be used, vs Object level automation).

Application Virtualization / Streaming

Application Virtualization is the concept of decoupling and isolating applications from the underlying Operating System (and each other), including all registry settings and filesystem changes. Depending on the technology, the applications can be cached and run locally, or “streamed” to the Desktop. Care should be taken to understand how these applications will behave in context of the Blue Prism environment (ie, will the application behave as if locally installed, as this may impact the development of any automation).

Application Layering

Application layering is similar to Application Virtualization in many ways, except that it allows for applications to be bundled within a virtual “stack”. In other words, the applications are no longer necessarily isolated from one another. Application layering technology usually enables the delivery of the Application layer via a proprietary agent and / or protocol. It is usually coupled with some form of User Virtualization.

User Virtualization / User Environment Management (UEM)

The implementation of a non-persistent Virtual Desktop strategy with Application Virtualization or Layering often also requires the decoupling of User personalization from the image, as user personalisation and customisation

would otherwise be lost after logout and / or reboot. This can be achieved in various ways, including use of complementary software such as VMware User Environment Manager, or Citrix AppSense.

Persistent / Non-Persistent Virtual Desktop

VDI Technology provides flexible mechanisms for delivering a desktop environment to a user. In general terms, this is via one of the following strategies:

- Non-Persistent - User is allocated a VM from a pool of VMs, which are based on a “linked clone” of a master image. This VM may be allocated from a pool of pre-provisioned VMs, or even created “on demand”, using techniques such as VMware’s “Instant Clone” technology. Use of non persistent VMs is almost always coupled with some form of Application Virtualization or Layering and User Virtualization / UEM. Non persistent VMs will normally be refreshed (recompiled) from the master image, either on boot, or periodically initiated by an administrator after the master image is updated.
- Persistent - A VM is created from a master image as a “full clone”. A user is allocated to the same VM on each logon. Any personalization and system changes are retained. This model is more predictable, but comes with a higher maintenance overhead.

3.3.2. Desktop Virtualization for Blue Prism – General Design Principles

The use of VDI / HVD for Blue Prism should be possible, as long as the environment is designed and operated within certain parameters and with a full understanding of the underlying technologies. The main general considerations are:

- Consider that the use of Desktop Virtualization is generally based on a design principle of a 1:1 mapping between user and desktop and often on the basis of “on demand” desktop provision. This can introduce some design challenges for the Runtime Resources – such as how the session will be initiated and remain persistent and available to the Blue Prism Control Room. It may also introduce complexity into the Development lifecycle – such as how workload can be shared between developers and how configuration changes are moved into production.
- VDI technology is often coupled with Application and User layering technology, which can introduce further complexity. Detailed guidance on these topics is provided in subsequent sections.
- Introducing desktop Virtualization software is often seen as attractive, as it can reduce management overhead, but it also introduces complexity and additional points of failure – the overall architecture for the VDI delivery solution needs to be considered against the non functional requirements for the Blue Prism solution, including Availability, Disaster Recovery and Security.
- The impact of any variables within the Virtual Desktop operating environment must be considered – for example, changes to IP addresses, which may impact the ability to access an external application.

3.4. Desktop Virtualization for Blue Prism – Quick Reference

The following tables may be used as a “quick reference” guide to each of the main desktop Virtualization topics, the key design considerations and suitability for the Blue Prism environment. **Refer to the “known issues” section for any issues or recommendations related to specific Virtualization platforms.**

✓ Fully supported

! May work, but be aware of the limitations

✗ Not supported

| | | |
|---|---|---|
| <p>Persistent Virtual Desktops</p> | Example Technologies | Citrix XenDesktop (Static Persistent option), VMware Horizon View (Dedicated User Assignment with Full Clones) |
| | Key Characteristics | <ul style="list-style-type: none"> OS Image is not periodically refreshed from Gold Image (full clones, not linked clones) User is assigned to the same VM on login Personalisation settings are retained |
| | Interactive Client | ✓ |
| | Runtime Resource | ✓ |
| | Login Agent | ! |
| Design Considerations and Limitations | <ul style="list-style-type: none"> Additional maintenance overhead vs non persistent Patching and update process must be carefully considered Application delivery mechanism may be different to existing corporate VDI strategy Login Agent is only supported on Xendesktop v7.6 and above (as 3rd party credential providers are not supported below this) | |
| <p>Non Persistent Virtual Desktops</p> | Example Technologies | Citrix XenDesktop (Static or Random non-persistent option), VMware Horizon View (Floating User Assignment and / or Linked Clones) |
| | Key Characteristics | <ul style="list-style-type: none"> OS Image may be refreshed on boot, or on scheduled basis. User is not guaranteed to be allocated to the same VM on logon User personalization is lost, unless coupled with additional technology Use of Login Agent or another mechanism for logging in the OS user automatically is required. |
| | Interactive Client | ! |

| | | |
|--|---------------------------------------|---|
| | Runtime Resource | ! |
| | Login Agent | ! |
| | Design Considerations and Limitations | <ul style="list-style-type: none"> Impact of Virtual Desktop image refresh must be carefully considered (for developers and runtimes) Consider how configuration changes required for a process / application will be captured and moved from Development through to production Other technology is often required to enable the portability of the operating environment for Developers and Runtimes. Login Agent is only supported on Xendesktop v7.6 and above (as 3rd party credential providers are not supported below this) |

| | | |
|---|---|--|
| <p>Presentation Virtualization / Hosted Shared Desktop</p> | Example Technologies | Microsoft RDSH, Citrix XenApp |
| | Key Characteristics | <ul style="list-style-type: none"> User is allocated a “published” desktop or application from a multi-tenant server System resources are shared between all sessions Sessions are not persistent |
| | Interactive Client | ! |
| | Runtime Resource | x |
| | Login Agent | x |
| | Application Automation | ! |
| Design Considerations and Limitations | <ul style="list-style-type: none"> Use of Interactive Client as a published application is possible for Control and monitoring only (not development) Automation of applications delivered via Presentation Virtualization may be possible, but will be limited to Surface Automation Techniques, which can add complexity and time to development. | |
| Application and User Environment Virtualization or Layering | Example Technologies | VMware App Volumes or Thinapp, Citrix XenApp, Unidesk, VMware User Environment Manager, Citrix AppSense, Microsoft App-V, Unidesk |

| | |
|--|---|
| <p>The diagram illustrates a multi-layered architecture. At the top, 'User Data' is shown in a dashed box, connected to a server icon. Below it are two 'App Container' blocks, followed by 'Layering / Streaming Technology', 'OS', and 'VM'. These layers sit on top of a 'Hypervisor' block, which is supported by hardware components like a CPU and memory modules.</p> | <p>Key Characteristics</p> <ul style="list-style-type: none"> • Application and / or User Personalization is isolated from the core image of a VM, via app Virtualization, layering and / or UEM technology. Generally this would be coupled with a non persistent VDI strategy. • Application and User customization are generally delivered via separate techniques or complementary technologies. |
| <p>Interactive Client</p> | <p>!</p> |
| <p>Runtime Resource</p> | <p>!</p> |
| <p>Login Agent</p> | <p>!</p> |
| <p>Application Automation</p> | <p>!</p> |
| <p>Design Considerations and Limitations</p> | <ul style="list-style-type: none"> • Consider how the user environment and application customisations required for a process will be captured and packaged with a process - from Development through to Production • Credential management approach will be critical (normally application and personalization is 1:1 – consider how this will be managed with the Runtime Resource OS credentials) • Consider how Developers will share workload (bearing in mind the 1:1 mapping of customization and application layers) • Consider how the Blue Prism Runtime Resource (and Login Agent) will be started after a reboot. Generally this means that the applications must be part of the base OS image, as most Application layering technology will only operate post boot (Unidesk is one notable exception). • Consider the overall impact on availability from additional components within the architecture – for example the application layering agent availability, application delivery Servers or database. |

3.5. Additional Virtualization Software

Once the primary Hypervisor and VM delivery technology has been selected, there are often many additional layers to defining a Virtualization strategy, including Orchestration, Monitoring, Control and Security. It is outside of the scope of this document to cover all of these topics and expected that an architect with Virtualization experience would be involved in the overall design of the environment. The following sections provide a summary view of any areas, where there may be a material impact on the design of the Blue Prism environment.

3.5.1. Software Defined Data Center Networking Virtualization (SDN)

Software Defined Networking products, such as VMware NSX and Cisco ACI, are being used in the cloud, or on premise, to provide an additional virtual network control layer (overlay) on top of the physical network. Considerations for implementing a Blue Prism environment on SDN are not fundamentally different to physical networking, however it is relevant to mention the following points:

- Refer to the Infrastructure Reference Guide to gain a full understanding of the required communication flows, when designing the SDN topology for the environment.
- Consider any performance impacts or variances that may be introduced by differences in the network topology from the current desktop operating environment – If users performing processes today are connected directly to a physical network, implementing the Robots on SDN may introduce performance variations or connectivity issues.

4. Designing the Virtualization Platform

4.1. Overview

Information about the design of the Virtual Host and suitability of each Blue Prism component for Virtualization is provided within the respective guide for each component below.

4.2. Host hardware requirements

In addition to the system requirements of the individual virtualized instances, the requirements of the underlying host system should also be considered. This will be an aggregated view, based on the expected demands of the planned Virtual instances. Consideration should always be given to the supported host failure scenarios. In other words, if the Virtual host platform is designed to allow the failure of 2 hosts within a cluster, then all hosts within that cluster must be designed with sufficient resources to host all business critical VMs, in event of 2 hosts failing.

4.2.1. System Resource Specifications for virtual instances

The hardware capacity that will need to be allocated to the virtual instances can be established once the number of instances of each component (Blue Prism Server, Runtime Resource etc.) have been decided. Minimum specifications for each component is provided in the Infrastructure Reference Guide.

Right-sizing of Virtual Devices is a complex area. Given the likely variable workload of the virtual workforce, it can be difficult to predict the ideal minimum specification at the design stage. As such, it is important not to over-allocate resources early on. Instead, the specifications should first be defined, based on all available data (OS + Blue Prism minimum specs + expected resource requirements from automated applications). As development and deployment is progressed, monitor and baseline the performance and capacity of the environment and adjust accordingly.

The following guidance should be used initially:

- **CPU Allocation**

There is no single reliable formula to determine the real vCPU to pCPU scaling factor. This topic is very dependent on the types of applications being run on the Virtual device and their ability to take advantage of performance efficiencies provided by the Hypervisor platform, the configuration of the Virtual host and other factors. It is important to recognise that a vCPU does not necessarily provide equivalent performance to a pCPU and build some flexibility into the design and as much as possible, under estimate vs overestimate.

- **Memory**

The amount of RAM allocated to a given virtual instance should be no less than that specified as a minimum requirement based on the type of Blue Prism component that is being configured. The minimum and recommended RAM for the operating system and managed applications being configured should also be taken into account. Often this is difficult to predict at the design phase, therefore it is recommended to consider pre-defined “tiers” of resources, to account for possible small, medium and large workloads.

Virtual instances **should not** be configured to share RAM. (E.g. the total amount of physical RAM available must comfortably exceed the total amount allocated to the virtual instances).

- **Disk Space**

The amount of available disk-space allocated to a given virtual instance should be no less than that specified as a minimum requirement based on the type of Blue Prism component that is being configured. The minimum and recommended disk space for the operating system and any managed applications should also be taken into account.

The disk performance should also be considered, particularly where a common disk subsystem is shared by multiple virtual devices. This consideration should take into account the third-party client applications that will be deployed onto the devices to enable automation as it is such applications that are responsible for the highest proportion of usage.

It is recommended to also follow any right sizing guidance provided by the Virtualization technology provider.

4.3. Dedicated vs Shared Physical Host Platform

The cost benefits of sharing the physical hosting platform (with other applications, or between Blue Prism instances) should be carefully balanced with the following considerations:

- Use of a shared host platform may make the identification of performance issues and application of patches more challenging.
- Consider the potential impact of a host failure or maintenance. This may have an impact on the overall availability or performance of the hosted Blue Prism environment.
- Use of VMware HA and DRS rules (or equivalent) should be considered to ensure adequate balancing and recovery of critical components between hosts.
- Use of separate physical hosts or clusters for Development / Test and Production should be considered. This decision will generally be driven by the requirements, such as availability and security.
- Consideration should be given to the disk subsystems used, especially if the Database server will be virtualized. Use of a shared disk subsystem in some cases may have a significant impact on performance.

Appendix A – Known Issues

The following section outlines any known issues or limitations with using specific Virtualization Technologies.

| Technology / Version | Impacted Blue Prism Component(s) | Issue and Recommendations |
|---|----------------------------------|---|
| Citrix XenDesktop (all versions prior to 7.6) | Login Agent | <p>Symptoms: Unable to log in user via Login Agent</p> <p>Issue: Login Agent is not formally supported at versions prior to Xendesktop 7.6, due to the lack of support for 3rd party credential providers.</p> <p>Recommendations: Use version 7.6 or above if Login Agent functionality is required.</p> |
| Citrix XenDesktop (all versions) | Runtime Resource | <p>Symptoms: Processes appear to “hang” during execution</p> <p>Issue: Citrix uses “hooking” to intercept windows API calls. This can cause deadlocks in certain applications, causing the symptoms above</p> <p>Recommendations: If Citrix is implicated in deadlocking the processes which have been uncovered by the Microsoft debug diagnosis, that one way to prevent such issues is to add a list of exclusions via a Registry key for CTXHook (Citrix Hooking).</p> <p>CTX Hook exclusions are found in the following locations:</p> <p>HKLM\SOFTWARE\Citrix\CtxHook</p> <p>HKLM\SOFTWARE\Wow6432Node\Citrix\CtxHook64</p> <p>HKLM\SOFTWARE\Wow6432Node\Citrix\CtxHook</p> <p>They each have a Key called "ExcludedImageNames" which can contain the executable names to exclude, e.g.:</p> <p>HKLM\SOFTWARE\Citrix\CtxHook\ExcludedImageNames = calc.exe,notepad.exe</p> |
| | | |