The real costs of VDI downtime and how to mitigate

Fact based calculations to validate your investment in a structural testing and active monitoring environment
Disclosure and Warranty

The information, concepts, and ideas contained in this document are the property of Login VSI. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Login VSI. Any product descriptions or representations in this document are for identification purposes only and are not to be construed as a warranty of specific properties or guarantee or warranty of any other type.

Login VSI shall assume no liability, either explicit or implied, for the documentation. Information in this document, including URL and other Internet Web site references, is subject to change without notice.

All sample code described in this document is provided by Login VSI for illustrative purposes only. These examples have not been thoroughly tested under all conditions. Login VSI, therefore, cannot guarantee or imply reliability, serviceability, or functionality of these programs or code examples. All brand names and product names used in this document are trademarks of their respective holders and are recognized as such.

© 2018 Login VSI. All rights reserved.
The real costs of VDI downtime and how to mitigate

Table of Contents

Management Summary .............................................................................................................................................. 3
  Key Findings .................................................................................................................................................. 3

1. Downtime in VDI ............................................................................................................................................. 4
   1.1 Defining downtime ............................................................................................................................. 4
   1.2 Planning for downtime ......................................................................................................................... 4
   1.3 Downtime dimensions ......................................................................................................................... 4

2. Productivity .................................................................................................................................................... 5
   2.1 Lost opportunity ................................................................................................................................. 5

3. Damage to reputation ................................................................................................................................. 7
   3.1 Cost of downtime calculations ............................................................................................................ 7

4. Identifying and resolving outages ............................................................................................................. 9
   4.1 Relying on users ............................................................................................................................... 9

5. Helpdesk time to resolution ..................................................................................................................... 11

6. Mitigating downtime .................................................................................................................................... 12
   6.1 Bypass helpdesk ............................................................................................................................... 12
   6.2 Resolve issues faster .......................................................................................................................... 12
   6.3 Reducing the length of outages ......................................................................................................... 13
   6.4 Identify future trouble spots with trending ...................................................................................... 13

7. Conclusion .................................................................................................................................................. 14
The real costs of VDI downtime and how to mitigate

Management Summary

Downtime is expensive. Downtime can be especially damaging in virtualized desktop environments where shared resources mean that downtime events are not isolated, but hit groups of users. The obvious loss is in employee productivity, and the salaries that are paid out even when employees can’t work. That’s the tip of the iceberg—what about lost opportunities or revenue when the business can’t reach customers, or the loss of reputation if you can’t deliver to your customers because of the outage?

There are the loftier objectives of operational efficiency and delivering a great end user experience. Then there is reality, the dark side of delivering a virtualized desktop environment where IT relies on users to notify them when desktops are “slow” or even unavailable. IT becomes reactive and spends time and resources following up on issues without having a good idea of the root cause. Without measurable, predictive performance, the risk of downtime rises.

We believe it is worthwhile for organizations to evaluate the costs of downtime so that they can determine investments for mitigating downtime and evaluate the return on investment for mitigation. Predictable, measurable virtualized desktop performance is an important step to proactively managing environments to the benefit of both IT and end user experience. Login VSI and Login PI are two such resources that reduce the risk of downtime in virtualized desktop environments.

This paper will explore how organizations can measure the impact of downtime and discusses specific risk mitigation efforts with Login VSI and Login PI.

Key Findings

For the average company, the cost of downtime in a VDI environment is $5000 per minute. Your cost could be higher or lower, depending on the scale of your VDI deployment. Salaries and opportunity costs require the VDI system maintaining uptime. With early warnings from Login PI, trimming 10 minutes of downtime from an outage could save the organization $100,000 per year.

Login VSI can help organizations optimize their VDI environments with realistic, real world workloads. When used as part of change management, Login VSI helps prevent downtime due to unexpected impact from updates and patches. Login PI used in the production environment notifies administration when there is a likelihood of unacceptable end user desktop performance. When used in combination, Login VSI and Login PI more than pay for themselves by preventing downtime.
1. Downtime in VDI

Organizations that incorporate desktop virtualization do so to increase security, improve manageability, and save costs. End user experience—productivity, application response time, flexibility—with the virtualized desktop environment is critical to the success of the VDI project, but is also critical to the business.

In virtualized desktop environments, two objectives rise to the top when infrastructure planning and architecting: high availability and delivering a great end user experience. This paper will address both sides of the coin, because both are essential to maximizing the promised benefits of VDI.

Many companies are adopting VDI or other Server Based Computing (SBC) technologies to deliver desktops or applications to their users for an experience that feels like—for the end user—a traditional client-server model. Whether in financial services, retail, or government, many of the user groups on VDI are customer-facing. When accessing the virtualized desktop is unavailable, the organization is impacted on many levels.

1.1 Defining downtime

We define downtime as a system that is unavailable to users for either seconds, hours, or something in between. Due to the complexity of VDI environments, downtime could be caused by over-allocation of shared resources, network issues and a myriad of other factors. High lag time or latency is effectively downtime and is common in virtualized desktop environments. While the lag may be measured in seconds or milliseconds, over time this can have an impact on productivity.

1.2 Planning for downtime

While we know downtime is expensive, and we’ll look at specific numbers shortly, it’s important for the organization to be clear about its goals on business continuity. For what duration of time is downtime acceptable, before the consequences are unacceptably damaging to the business. The Recovery Time Objective attaches duration of downtime to the business process. Once this is determined, HOW exactly this recovery time will be shortened still needs to be investigated.

1.3 Downtime dimensions

Calculating downtime for each organization requires looking across productivity, opportunity, and reputation.

No two businesses are alike, and every company puts different weight on the cost of loss associated with each of these. This paper will make very conservative estimates of costs based on an average cost across many industries. The purpose of presenting this cost is to start a conversation in your organization about your specific situation. Do most of your company’s risks lie in productivity or in reputation? Are they internal or external-facing, or a mixture of both?
2. Productivity

Productivity tied to end users not being able to work for an extended time (true downtime) can be calculated by the cost of the wages multiplied by the lost output or lost revenue. This is a relatively straightforward calculation. The obvious cost is the salaries of employees—they still get paid while not able to work because the system is down. It gets more complex when the salaries of various employees are factored in, especially when there is a wide discrepancy (seasonal workers versus professional staff).

There are other costs though, depending on the nature of the outage, such as costs associated with overtime for support staff working on a resolution, or support costs related to bringing in special expertise for an issue.

Productivity is not limited to end users. Unexplained downtime and unmeasurable performance impact IT-productivity and efficiency. Chasing help desk tickets when end users say the system is slow, and trying to perform root cause analysis based on subjective inputs puts IT into an inefficient state. IT spends six times more effort in a reactive mode over a proactive mode.

2.1 Lost opportunity

Lost opportunity costs are harder to track down. Did your team lose sales because they could respond to customers or business opportunities? Also tied to the third category of reputation lost, what about lost future revenue because of a bad customer service experience a customer had, because your team could work with them while the outage occurred? These are harder to measure, but can be directly impacted by downtime.
Lost opportunity can attempt to be measured by looking at growth on a year over year, month over month basis, then determining the metric of growth. Averaging the growth per hour, or even to the minute, will be a rough estimate of opportunity lost because of downtime.

The SVP of IT at a national financial advisory services group said that his lean and efficient team learned that proactive management of the virtualized desktop environment is a 6:1 ratio—reactive time to proactive management for the level of effort.

By becoming proactive about managing performance in their virtualized desktop environment, the technology team at Wealth Management puts every dollar saved back into the business to fuel growth.
3. Damage to reputation

Reputation has internal and external dimensions. When customers depend on and trust a company, downtime has a significant impact. Any form of downtime can make a customer lose confidence: “How is this financial company going to keep my money safe if they can’t even keep their computers running?” Brand equity measures brand value, but there is no agreement on a qualitative way to measure brand equity. We know the brand is critical, maybe the most important aspect of the business, but the measure of its value is amorphous. What’s more, knowing exactly what the impact of loss of trust has would need to factor in the set of stakeholders who experienced the downtime, how public was the event, how well and quickly did the company restore confidence.

Within the organization, downtime can be damaging to the reputation of the IT organization. Executives lose confidence in IT’s ability to understand and fulfill business needs. Budgets get more scrutinized, then cut, then alternative solutions (and people) are sought. From end users, loss of confidence can turn workers into skeptics. Complaints about the system being slow can be largely due to perception, rather than actual lag times.

You just rolled out an additional 500 new users to your virtualized desktop environment for seasonal help. You tested the environment with a smaller number of users.

In other words, you cut corners and did not test at scale. When the boot storm hits, no one can answer customer calls for 15 minutes for 500 users. You didn’t see it coming, so your recovery time was slow.

How much did this cost your business in terms of lost revenue? Lost opportunity? Lost reputation?

3.1 Cost of downtime calculations

We explored the main categories of the business that downtime affects—productivity, lost opportunity, and reputation. These help us understand the impact of downtime, but let’s step out and look at what industry analysts have found looking across these dimensions in various industries and company sizes.

There are many estimates of what downtime costs a company, and they vary based on the size of the company and what systems are down. Here is some of the estimates we found in our research:

1. Ponemon Institute Research did a study of multiple datacenters, and estimated the average cost of datacenter downtime was approximately $7,900 per minute, and the average incident length was 86 minutes (Ponemon.org, Cost of Data Center Outages 2013).
2. CIO Insight found that when systems are down, employees are only able to work at 63% efficiency (cioinsight.com, IT Downtime Carries a High Pricetag).
3. Gartner makes a very conservative estimate at the hourly cost of downtime at $42,000 (networkworld.com, How To Quantify Downtime).
4. Enterprise Management Associates puts the cost of application downtime at $45,000 per hour, averaged across low mid-tier to large enterprises (zdnet.com, Real Cost of Application Outages).

Based on these reports, we can see that there’s little consensus on what downtime actually costs, but we can use this to come up with some conservative estimates. The Ponemon numbers are the most...
The real costs of VDI downtime and how to mitigate

referenced and have the most backing data, so we’ll work with this, and we’ll use the CIO Insight research to assume users can still work at 63% efficiency while systems are down—good employees will still find ways to do their job, so this conservative result bakes in some user ingenuity into the equation.

Using these guidelines, we’ll assume at a VDI outage costs a company, on average, $5,000 per minute of downtime.

**DAN POTHIER, SVP Technology at WEALTH ENHANCEMENT, a national financial advisory services group, said that his lean and efficient team has learned that proactive management of the virtualized desktop environment is a 6:1 ratio – reactive time to proactive management for the level of effort.**

Your creative team is the newest set of end users to be part of your VDI environment. When Harry wants to collaborate using Illustrator and Photoshop, the team experiences lag time and gets frustrated. They ditch their work desktops for their personal Macs and decide to share files via their personal emails. They let you know that “VDI isn’t working” casually while waiting for the coffee to brew.
4. Identifying and resolving outages

Black boxes. Routers down. What is the root cause? A VDI deployment can be one of the most complex architectures in an IT environment. Uptime requires that every component of the VDI stack—storage, compute, network, applications—be up and running as expected. An outage of any component will likely mean the entire system is effectively down.

Capacity planning for VDI is critical in reducing outages. A system that is heavily oversubscribed can be effectively offline. If it takes users several minutes to log in, and apps take several seconds to respond to activity, then you’ve got a system that users can’t use and are effectively offline. These types of outages are hard to detect: Your operations management console may show you that all VDI services are up and running, but very few Ops consoles can tell you the relative health of the system.

The measurements taken by most monitoring tools don’t always paint a clear picture of the performance of a system. Most tools can report high CPU usage, but it’s not always clear what that means. High CPU usage on a session broker may be a non-issue, as most interactions with the broker last less than a second, it’s likely not a large bottleneck on performance. High CPU on an SBC/Remote Desktop Services (RDS) computer might mean all users on the system are experiencing a degraded performance. It might not be indicative of anything other than a highly efficient, well-sized system that is delivering a great user experience for all users on the server. Relying on performance counters to identify outages will likely result in many false positives, where administrators are notified of high levels of consumption, but without any indication of whether users on the system are impacted.

There are a few outage scenarios that are unique to VDI/SBC environments that are equally hard to detect. One is the “black hole” server where the RDS/Citrix/SBC server appears to be healthy—it’s responding to pings and is accepting new logon requests — but the sessions never actually start a desktop. The server has just gone dark and isn’t delivering sessions, though it seems healthy from the monitoring tools. There are also external outages that are hard to detect—a gateway that is responding to pings internally, but may not be responsive on the external network. This would also appear to be up and running, but in reality, users connecting from outside the corporate network will be unable to do so.

For many customers, the most reliable way to determine if the system is up, is to rely on end users to call and report these issues. This is inherently a poor method, for a variety of reasons.

4.1 Relying on users

The reality is that many virtualized desktop environments with application performance management and application performance monitoring software still rely on end users to experience the downtime to identify an issue. 32% of customers rely on end users to notify them of app performance issues. Furthermore, 80% take up to 4 hours to repair an outage (see VMblog: Manage Engine report).

Many customers report that the most effective way to determine if their VDI/SBC system is down, is to wait for users to call the helpdesk. There are important reasons why end users make for a poor notification system.

Even with monitoring software, 32% of customers rely on end users to notify them of app performance issues.
First, users have a subjective understanding of their desktop performance. Secondly, users are not the best to judge whether an outage is critical or not. Many users, faced with a system they can’t log in to first thing in the morning, may take this as an opportunity for time to grab a cup of coffee, socialize with coworkers, or otherwise take advantage of an unexpected break from work for a few minutes. They may assume that someone else has already started the (potentially tedious) process of calling the helpdesk, opening a ticket, troubleshooting their connection, and waiting for the outage to be escalated.

Eventually, someone will decide they must get work done and report the outage.
The real costs of VDI downtime and how to mitigate

5. Helpdesk time to resolution

Calling the helpdesk is just the start of the outage resolution process. There will be several steps that helpdesk must go through to troubleshoot the problem, so it can still take several minutes from when a user calls in until the problem is verified and resolution can begin.

Is there a queue to speak to the helpdesk? If all helpdesk agents are already on calls, a user calling to report the VDI outage may have to wait several minutes for the next available agent.

Once an agent takes the call, they likely should open a trouble ticket. This may take a few minutes to enter the name and contact details of the caller, and document the purpose of the call.

The helpdesk agent should verify the scope of the outage—does the issue reside just with this caller (caller is unable to get on the internet where they are located) or does it affect a subset of users (the external gateway is down, so only users on the corporate network have access) or does it affect all users (broker is down, no new connections to the VDI environment can be created). Determining this typically requires going through a troubleshooting script to reboot the machine, verify network connectivity, etc. It may take several more minutes to verify that the outage appears to extend beyond just the caller.

By the time a determination is made that there is a widespread outage, several minutes may have already passed. That’s just to the start of the resolution process, which will include several more steps to identify which component has failed and what it will take to get it back on line. This could be as short as a few minutes to reboot a crashed server, or much longer if components must be replaced.

How much has that time cost your organization?
With DaaS growing in popularity as an alternative deployment method, (50% of new VDI users will be deployed on DaaS platforms, up from less than 5% today), responding to helpdesk tickets is still the responsibility of the client. (Gartner, “Desktop Virtualization with Power the Digital Workplace, 13 October 2015.)
6. Mitigating downtime

A key path to reducing downtime and the costs to the business from downtime is to use tools that help IT address performance proactively. Login VSI and Login PI can be used throughout the VDI lifecycle to help the IT department deliver higher availability and a better virtualized desktop experience by providing measurable and actionable data on end user performance.

In capacity planning your VDI environment, whether greenfield or expanding an existing system, it is important to benchmark user performance and perform stress tests. Login VSI uses realistic user workloads to determine how many users can be supported with any given configuration. The measurement used is VSImax. Using Login VSI in planning and change management to production environments is an important step in mitigating that downtime will happen because of overcapacity.

The next important measure to mitigate downtime risk and reduce the amount of time of outages if they happen is to deploy Login PI. Login PI works by simulating real end users accessing your VDI environment and tells administrators ahead of time when end users experience performance issues. When the Login PI virtual user finds the desktop is performing outside of expected parameters, it instantly notifies IT administration.

Unlike performance metrics that may or may not directly impact the user experience, Login PI will report exactly what real users are experiencing. A notification that a server is at 100% requires an administrator to research and determine what, if any, action must be taken. In contrast, a Login PI notification will tell you that logins are taking much longer than expected, or applications are failing to launch. Login PI will send these notifications immediately—not after getting another cup of coffee and waiting on hold with the helpdesk.

6.1 Bypass helpdesk

Login PI runs a set, predictable workload on a schedule that IT administration specifies. Because it performs the same operations every time, it’s easy to establish a baseline of what expected performance should look like. Administrators have full control over what kinds of performance they want to be notified of. For example, you may want to be alerted any time an application’s launch time exceeds the average by 50%. An admin may only want to see alerts for slow logon time if it exceeds five minutes, regardless of what the typical reported login time average is.

IT admins can be immediately notified when the service level exceeds acceptable levels. There’s no waiting for users to call and complain to the helpdesk and for the helpdesk to escalate.

6.2 Resolve issues faster

Login PI can trigger more than just alerts when outages and slowdowns are detected, it can prompt other automated actions too. Login PI can automatically restart, notify, and other actions to quickly resolve issues. One typical scenario might be a broker service that occasionally hangs and stops responding, and the fix is to reboot the server. When Login PI detects that logons are failing, it can trigger a PowerShell script to reboot the failed server.

Imagine the whole chain of events that normally should happen: users noticing the outage, calling the helpdesk, helpdesk logging the ticket and notifying an IT admin and the IT admin initiating the server reboot—a several minute process, reduced to seconds, with no human interaction. The reduction in outage times could be significant.
6.3 Reducing the length of outages
Since we know the cost of outage time in minutes, we can do some simple calculations to determine how much downtime we can reduce. For purposes of this exercise, we’ll estimate that Login PI will reduce outages by 10 minutes—roughly the time taken by employees to wait around to see if the problem gets resolved, then calling the helpdesk, and the helpdesk puts in the escalation to IT.

Reducing that outage by 10 minutes by bypassing the standard helpdesk escalation procedures is a resulting $50,000 per outage a company potentially saves in lost productivity and opportunity. That’s just for one outage, most companies estimate they see two unplanned outages per year.

Trimming 10 minutes from outages could save $100,000 per year by using Login PI.

6.4 Identify future trouble spots with trending
In addition to real-time notification of outages, Login PI can also help you identify performance trends that could be potentially leading up to an outage or degraded employee performance. Login PI can help you see trends like long login times. Are your user profiles taking increasingly more time to load? Login PI can help you see those login times. With Login PI you can identify the times of day or days of the week when performance is most degraded, so you can plan for added capacity accordingly.
7. Conclusion

Unplanned downtime is a critical cost for organizations, costing companies an estimated average of $430,000 per year, besides the many costs that are unquantifiable such as reputation loss and opportunity loss. Using Login VSI and Login PI gives organizations measurable, actionable data about the virtualized desktop environment that are used to increase uptime, right-size capacity, and understand the impact of changes that could affect end users.

Using Login PI to monitor the uptime and performance of a VDI environment can reduce the time to get a resolution for outages by reporting them more accurately and quickly, saving companies up to $50,000 per outage with an average of two outages per year.

Learn more

To find out more about the VDI Lifecycle, Login VSI or Login PI, please visit www.loginvsi.com. To schedule a demo, contact us at sales@loginvsi.com
The real costs of VDI downtime and how to mitigate

Disclosure and Warranty
The information, concepts, and ideas contained in this document are the property of Login VSI. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Login VSI. Any product descriptions or representations in this document are for identification purposes only and are not to be construed as a warranty of specific properties or guarantee or warranty of any other type.

Login VSI shall assume no liability, either explicit or implied, for the documentation. Information in this document, including URL and other Internet Web site references, is subject to change without notice.

All sample code described in this document is provided by Login VSI for illustrative purposes only. These examples have not been thoroughly tested under all conditions. Login VSI, therefore, cannot guarantee or imply reliability, serviceability, or functionality of these programs or code examples. All brand names and product names used in this document are trademarks of their respective holders and are recognized as such.

©2018 Login VSI™ is a trademark of Login VSI, Inc. and Login VSI, B.V.