White Paper

3 ways to get more from Citrix Virtual Apps and Desktops with Citrix Director

Citrix Director is your console for day-to-day management and monitoring of Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop), including viewing and controlling user sessions, reporting on environment usage, and notification and alerting.

Let’s explore the three key ways you can use Director to get more from your Citrix solution.

1. Simplify troubleshooting and user actions to increase admin productivity

As you're getting started with Director, you'll find numerous features to help you monitor overall system health, track user activity, and streamline administrative tasks.

Application analytics

The Applications view in Director provides an overall picture of the health and real- time usage of all published applications. Typical use cases for this feature include:

- **Top Running Applications (default view)** – This is the default view; you can get more details by navigating to **Application Instances** in the **Filters** view.
- **Application Health** – Check the Faults and Errors count over the last hour to see how each app is performing, and then drill down to **Application Failures** in the **Trends** view to see the reasons for failures and the VDA machines on which they've appeared.
- **Search Application** – Check the health and usage for a specific app.

You can get more details on this feature here.

Shadow users

To work directly on a user's connected virtual machine or session, first verify that the user is connected to the machine you want to shadow by checking the machine name listed in the user title bar. Then:

- In the **User Details** view, select the user session.
- Activate shadowing for the selected user session:
    - For machine monitoring, in the **Activity Manager** view, click **Shadow.**
    - For session monitoring, in the User Details view, locate the **Session Details** panel and click **Shadow.**
- After the connection initializes, a dialog box prompts you to open or save the **.msrcincident** file.
- Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
- Instruct the user to click "Yes" to start the machine or session sharing. For additional control, ask the user to share keyboard and mouse control.

Streamline Microsoft Internet Explorer browsers for shadowing

To configure Internet Explorer to automatically open the downloaded Microsoft Remote Assistance (.msra) file with the Remote Assistance client, enable this setting in the Group Policy editor:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Automatic prompting for file downloads.

Disconnect or restore a session

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server. You can use the **Session Details** panel of the **User Details** view to troubleshoot session failures and then take actions such as:

Action	Description
End applications or processes that are not responding	Click the **Applications** tab. Select any application that is not responding, and click **End Application**. Similarly, select any corresponding process that is not responding, and click **End Process**. Also, you should end processes that are consuming an unusually high amount of memory or CPU resources, which can make the CPU unusable.
Disconnect the Windows session	Click **Session Control**, and then select **Disconnect**. This option is available only for brokered Server OS machines. For non-brokered sessions, the option is disabled.
Log off the user from the session	Click **Session Control**, and then select **Log Off**.

More information:

- To learn more about creating hosting connections, see Connections and resources.
- To learn more about configuring the alerts in Citrix Hypervisor, see XenCenter Alerts.
- To learn more about configuring the alerts in VMware vSphere Client, see Working with Alarms.

Hypervisor monitoring and proactive alerts

To ensure the health of user sessions, it's important to know when a host may be experiencing some event, condition or state that could affect the machines running on it. Director gives you an at-a-glance view of all the hosts and any related alerts in your Citrix Virtual Apps and Desktops deployment so you can assess whether user issues are host-related.

To enable hypervisor monitoring, make sure you've created hosting connections to the hosts in your deployment as defined by Citrix Studio; only these connections will be monitored for the hypervisor alerts you've set up in Citrix XenCenter or VMware vSphere Client.

A prebuilt, modifiable Hypervisor Policy is available under Site Policy to monitor the connections. To learn more, see Hypervisor Monitoring and Proactive Alerts in Director.

Send a message

Director lets you send a message to a user connected to one or more machines. This can be useful for real-time notifications of impending desktop maintenance, machine logoffs and restarts, profile resets, and so on. Here's how to do it:

- In the **Activity Manage**r view, select the user, and click **Details**.
- In the **User Details** view, locate the **Session Details** panel, and click **Send Message**.
- Type your message information in the Subject and Message fields, and click **Send**.

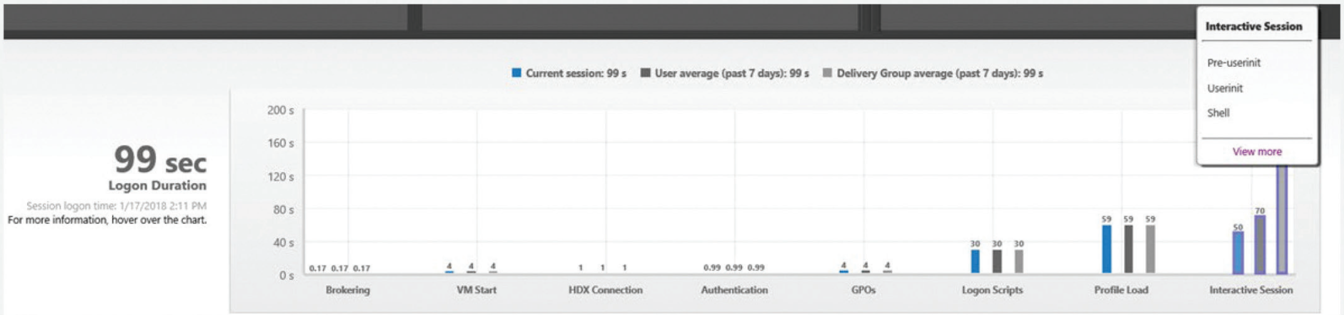
2. Optimize logon times to improve user experience

Launching apps and desktops with near-native performance can improve productivity and user satisfaction. As your environment grows and complexity increases, Director provides tools to dive in to the various session startup tasks, helping you optimize your environment. The first step is to understand the sequence of executions being processed:

- **Brokering** – Time taken to decide which desktop to assign to the user.
- **VM start** – If the session required a machine start, this is the time taken to start the VM.
- **HDX connection** – Time taken to complete the steps required in setting up the HDX connection from the client to the virtual machine.
- **Authentication** – Time taken to complete authentication to the remote session.
- **GPOs** – If Group Policy settings are enabled on the virtual machines, this is the time taken to apply group policy objects (GPOs).
- **Logon scripts** – If logon scripts are configured for the session, this is the time taken for the logon scripts to be executed.
- **Profile load** – If profile settings are configured for the user or the virtual machine, this is the time taken for the profile to load.
- **Interactive session** – This is the time taken to hand off keyboard and mouse control to the user after the user profile has been loaded.

(Note that logon duration is measured only for initial connections to a desktop or app using HDX, not for users trying to connect with RDP or reconnect from disconnected sessions.)

Figure 1: Login Duration panel in the User Details view



99 sec

Logon Duration

Session logon time: 1/17/2018 2:11 PM

For more information, hover over the chart.

In the User Details view, Logon Duration is displayed together with the time it occurred and a graph of the phases of the logon process (Figure 1).

As users log on to Citrix Virtual Apps and Desktops, the Monitor Service tracks the phases of the logon process from the time the user connects to the time when the desktop is ready to use.

Breaking down the longest step in the logon process: Interactive Session

Interactive Session is typically the longest phase of the logon process. It includes three sub-phases:

- **Pre-userinit** – This sub-phase overlaps with Group Policy Objects and scripts, and can be reduced by optimizing the GPOs and scripts.
- **Userinit** – When a user logs on to a Windows machine, Winlogon runs userinit. exe. Userinit.exe runs logon scripts, re-establishes network connections, and then starts Explorer.exe, the Windows user interface. This sub-phase represents the duration from the start of Userinit.exe to the start of the user interface for the virtual desktop or application.
- **Shell** – In the previous phase, Userinit starts the initialization of Windows user interface. The Shell sub-phase captures the duration from the initialization of the user interface to the time user receives keyboard and mouse control. The total logon time is not an exact sum of these phases, as some phases occur in parallel, and some phases include additional processing that might result in a longer logon duration than the sum.

The time taken for each of the three sub-phases is displayed in the interactive session bar as a tooltip. The cumulative time delay between the sub-phases and a link to the documentation is also provided.

How to use logon duration information to troubleshoot user logon issues

- To identify unusual or unexpected values in the graph, compare the amount of time taken in each phase of the current session with the average duration for this user for the past seven days, and the average duration for all users in this Delivery Group for the past seven days.
- From the User Details view, troubleshoot the logon state using the Logon Duration panel. If the user is logging on, the view reflects the process of logging on. If the user is currently logged on, the Logon Duration panel displays the time it took for the user to log on to the current session. Examine the phases of the logon process.
- Escalate as needed. For example, if VM startup is slow, the issue could be in the hypervisor, so you can escalate it to the hypervisor administrator. If brokering time is slow, you can escalate the issue to the Site administrator to check the load balancing on the Delivery Controller.

For in-depth documentation on using this feature, see Logon Performance – Interactive session drill-down.

Group policy processing breakdown

The logon duration panel in the user and session details view shows GPO duration, the time taken to apply the GPOs on the VM during the logon process. For details on the processing of each policy as a Client-Side Extension (CSE), including time taken and any errors or warnings, click on Detailed Drilldown in the tooltip in the GPO bar. The contents of the table in the dialog box can be copied for sharing or future reference. For more details, see Logon Performance – GPO drill-down.

User profile insights

Profile load is one of the most critical phases for logon duration, including the time needed to load a user's registry hive (NTUser.dat) and user files. To see detailed insights related to user profiles, hover over the **Profile Load** bar in the **Logon Duration** chart on the **User Details** page. The **Detailed Drilldown** button on the tool- tip will provide further insights to help you fix common load issues. For example:

- Use the Number of Large Files metric to identify users who should remove excess files in their user profile, and then use the Send Message feature on the User Details page to suggest that they do so.
- Use the Reset Profile panel in the Personalization panel in the case of extremely large profiles.
- Consider using features such as profile streaming and folder redirection to address systemwide profile load issues.

3. Proactively detect and resolve issues to keep users productive

Application probing is a key element of proactive monitoring, an approach focused on identifying and fixing issues before they interfere with user productivity.

Instead of learning about launch issues only through support tickets, by which time users are already unable to perform their tasks, admins can verify the health of critical applications well before the start of business each day to ensure a smooth and productive start for users.

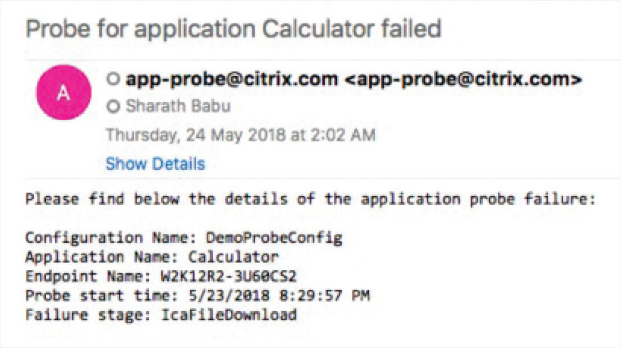
Application probing makes it possible to proactively monitor the health of an application while also effectively test the Citrix infrastructure through which it is delivered on a component-by-component basis. An agent installed on a user's machine launches the configured app and reports on its health to Director, which displays the results of all the probes in your site in a column on the Application Analytics table. Click on an individual probe to see the Application Probe Results page, which provides in-depth options to analyze the application's health.

The probe agent breaks down an application's launch to five stages: StoreFront reachability, StoreFront authentication, application enumeration, ICA file download, and application launch. This breakdown provides a deeper understanding of any issues that have arisen and facilitates root cause analysis related to application launch failures. You can then troubleshoot issues related to the applications, hosting machine, or connection before the users experience them.

Auto-alerts

Rather than having to log on early each day to monitor probe runs, admins can configure auto alerts to receive email notifications whenever there is an application launch failure. Application probes can be scheduled to run during off- peak hours across multiple geographies.

Figure 2: Sample email alert



Probe for application Calculator failed

○ **app-probe@citrix.com <app-probe@citrix.com>**
○ Sharath Babu
Thursday, 24 May 2018 at 2:02 AM
Show Details

```
Please find below the details of the application probe failure:

Configuration Name: DemoProbeConfig
Application Name: Calculator
Endpoint Name: W2K12R2-3U60CS2
Probe start time: 5/23/2018 8:29:57 PM
Failure stage: IcaFileDownload
```

The sample email alert above (Figure 2) contains information about the application name and failure stage, which helps the administrators start performing root cause analysis even before access to the environment is available for faster resolution.

For more details on configuring this feature, see Application probing.

For admins managing a large number of sites, manual agent installation and configuration can become time consuming. Power-shell scripts make it possible to automate this process to save time and effort. For a sample script, see the last section of this article on Application Probing – Your proactive application monitoring solution from Citrix Director.

Conclusion

We hope you find Citrix Director useful for managing and monitoring Citrix Virtual Apps and Desktops. By leveraging Director to analyze your environment, you can improve overall performance and user satisfaction to ensure full value for employees and the business. For ongoing updates on new features, subscribe to Citrix blog posts.

You can also find complete product documentation here.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States