

Access Control for Hosted Desktops

Hosted Desktop Connection Broker

Hosted Desktop Access Control

Each end-user has access from their web browser, fat, or thin client, to their remote Windows Desktop running on a centrally-Hosted Machine.

Single Sign-On

With the Leostream Connect Client for Windows 2000, XP, and Vista, users simply enter their username and password and are automatically assigned and logged into their remote Windows session. When they close their remote session they are automatically logged-off from the Connection Broker. Leostream Connect also provides progress reporting—for example, informing a user that their Hosted Desktop is currently booting.

Virtual Desktop Pooling

Users can be assignment a Hosted Desktop for a preset period of time. When the time period expires then the Desktop is returned to the Pool. This ensures a constant end user experience without wasting unused Desktops.

Virtual Desktop Failover

Leostream checks the state of Hosted Desktops before assigning, or re-assigning, them so if a Hosted Desktop fails then it is automatically replaced by another from the same Pool. So the failure of a host server would only cause limited disruption - the user would simply re-authenticate and be assigned a new Hosted Desktop.

Session Stickiness

The assignment of a particular Hosted Desktop to a user can be permanent, or just for a preset period of time. Ensures that users keep their Desktop even when there is a network interruption—but Desktops are not tied up unnecessarily.

Thin Client

Tight integration with thin clients such as the Neoware e140 with Linux or XPe and the Wyse S10-VDI, S30 Linux, and S90 XPe, provides a secure and seamless end-user experience.

Secure Access

Authentication and RDC session can be secured using SSL certificates - ensuring data security.

Dynamic Management of Hosted Desktop State

The VM state can be automatically changed when assigned and un-assigned, so allowing unused VMs to be kept in a powered-off state economizing both licensing and hardware utilization

Multi-Protocol Support

Remote desktop protocols supported include; Microsoft's RDP v5.0, Citrix's ICA, VNC, RAdmin, and VMware Remote Viewer—enabling the use of Linux and Windows 2000 and XP Hosted Desktops.

Policy Based Session Variables

Each access Policy can set the session variables, such as screen size, independently for each client type (Web, Fat, Thin). Furthermore, variables such as printer assignment can be determined by client location.

Monitoring and Reporting

Real-time monitoring of RDC sessions, and reporting via email and SNMP. Provides a more reliable monitoring solution because it takes into account the state of the Hosted Desktop.

[More ... >](#)

External Authentication

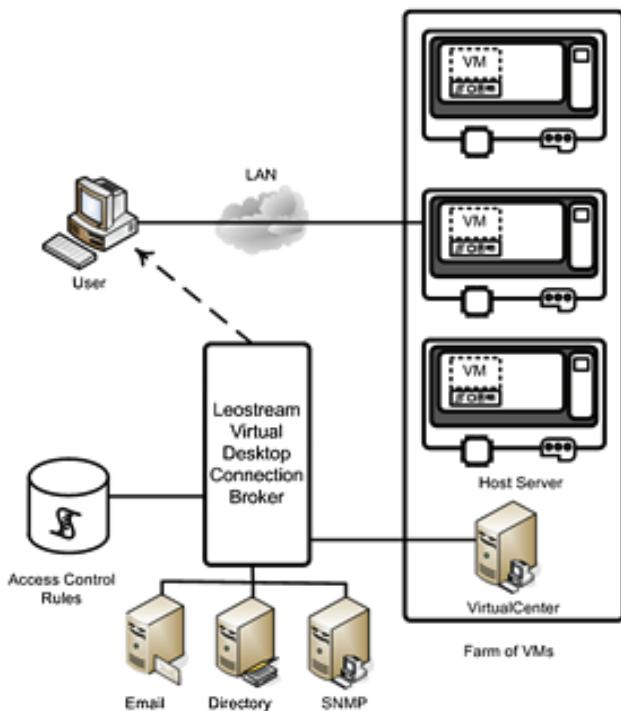
Users can be authenticated and profiled using Active Directory or LDAP servers without a schema change, so the introduction of Hosted Desktops does not require changes to the existing authentication system

User Activity Monitoring and Reporting

User status is displayed, user activity is logged, and users can be logged out of the system, so providing a central view of all user activity.

Virtual Appliance

The Connection Broker is distributed as a Virtual Appliance so it can be rapidly setup, duplicated, moved, and backed-up. It requires a minimum of 1.5G of Memory, and bridged network connectivity. CPU utilization is dependent on the Connection Broker load and will require between 1/10 and all of a 2GHz Xeon processor.



Interfaces

The Connection Broker provides external interfaces for: VMware VirtualCenter 1.4 and 2.0, Microsoft Active Directory, LDAP, XML-RPC control and client API, Controller logging, ODBC, Live Web Query and SNMP.

Scalability and Failover

The Connection Broker can be deployed as a single Virtual Appliance complete with its integrated database, or with a separate database. The integrated version can support up to 20,000 Hosted Desktops and up to 20 VirtualCenters.

The separated version can be scaled out with up to 128 Connection Brokers load balanced with a DNS load balancer and connected to a central database. This arrangement will scale to over a million Hosted Desktops.

Deployment

Download the Virtual Appliance, register it with the virtualization software, start it, and point it at the relevant VMware VirtualCenters and authentication server. You can now start to define access control policies.

More Information

Request a demo or free trial at www.leostream.com, or call +1 781 577 9584.

The screenshot shows the Leostream web interface with a table of VirtualCenters. The table has columns for Actions, Name, Status, Location, Language, and VirtualCenter. There are 5 rows of data.

Actions	Name	Status	Location	Language	VirtualCenter
Select	VirtualCenter 2.0	Running	All	All	VirtualCenter 162
Select	NF2-W2K12	Running	East	Spanish	VirtualCenter 162
Select	CPAQ2K3	Running	West	Spanish	VirtualCenter 162
Select	W2K3055SMALL	Stopped	East	English	VirtualCenter 162
Select	W2K-3055-4DS	Stopped	South	Spanish	VirtualCenter 162

5 rows

Customize
Click on the column headings to sort the list.

VMware, GSX Server, ESX Server, and VirtualCenter are trademarks of VMware, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. All other marks and names mentioned herein may be trademarks of their respective companies.