activu

vis|ability

on Your Network

Recommendations for network/system integration

5/15/2023
vis|ability v6.5

This document is designed to assist both Activu and the customer with requirements and recommendations for Activu integration on a client-provided system and network infrastructure. Please contact your Activu Implementation Team for additional information on the items below.

Activu Corporation • 301 Round Hill Drive • Rockaway, New Jersey 07866 • 973-366-5550 • www.activu.com

Table of Contents

Overview

The following are recommendations and guidelines for Activu implementation into an existing network infrastructure.

Windows Server and Desktop Operating System

Activu must run on Microsoft Windows operating system. Mac OS, Linux, and UNIX based operating systems can be leveraged as network sources using VNC or other commercially available clients and applications. Alternatively, endpoints may be configured as video capture encoded to video stream, instead of network capture sources.

Bandwidth

Formal bandwidth recommendations are dependent upon each client’s specific usage requirements and Activu’s customized design. Where there is a question of availability of provisioned network resources, Activu can provide sufficient details, based on a deployment/design, bandwidth needs for good performance. Generally, switched gigabit ethernet with reasonable (100Mbit) bandwidth to all endpoints should, in general, be sufficient. Availability and use of multicast can have a material benefit for video-intensive applications.

See Appendix A for more information.

IP Addresses

vis|ability uses fully qualified domain names as addresses for communication between its servers and network-attached devices, but where DNS stability or performance is an issue, static IP addresses. Workstations running client-side software from Activu, e.g., Desktop Client and Capture Client, may use static or dynamically provided addresses.

Network-attached devices

This section refers to NON-windows-based devices that would be attached to your network. This includes but is not limited to video encoders, RS232 control devices, audio equipment, network-attached storage, etc.

Video encoders have a variety of streaming options. The preferred method is using Multicast via RTSP H.264. Depending on the design and use case of the solution, this multicast traffic would be broadcasted onto your network.

Encoder cards that are installed in Display Nodes (Matrox IPX) will have a secured Telnet service enabled on port 23 that is needed for configuration.

Verify DNS Health and Functionality

Activu generally requires DNS. In the event, Activu Capture Client will be defined by hostname, or if Web sources will be leveraged in an Activu-driven display then the DNS configuration must be verified as functional and healthy.

Port and Protocol Configuration

The vis|ability platform is dependent upon specific ports and protocols. Network and desktop security allowances must be configured for this traffic to traverse the network and communicate with host systems. A list of the specific port and protocol allowances can be found below.

See Appendix B for more information.

Access to IT staff

The Activu team will need to interface with network engineers, administrators, technicians, as well as client-side personnel who are thoroughly familiar with the client's network operation, architecture, procedures, and policies.

Endpoint Security

Activu recommends that existing client security software be provisioned for vis|ability servers and all workstations that will run vis|ability software. This includes anti-virus, IPS, etc.

It has been observed that certain endpoint security software can impact the overall performance of a system (CPU/GPU), certain considerations for removal and exceptions may be required.

VLAN and Networking

We recommend that our servers be placed in the same VLAN or subnet as any source we will leverage, including network and decoder sources, this architecture simplifies network design and does not require opening ports outside the VLAN. However, it is critical that communication traversing VLAN's, subnets or sites is configured correctly (opening appropriate ports and protocols) for general network communication with vis|ability software system.

QoS

Activu does not need specific QoS configuration. However, Activu would need to be aware of any QoS policies implemented on specific routers/switches/VLANs/etc. that Activu would be interfacing with.

Administrative Rights for Installation

For Windows, Local or Network Administrative rights must be available at the time of the installation of vis|ability software of client machines.

Supported Operating Systems

Activu vis|ability software is supported only on Windows-based operating systems. The support operating system is as follows.

- Windows 10 Professional and LTSC
- Windows 11 Professional
- Server 2016, Server 2019, and Server 2022

Operating System Prerequisites

This section applies to OFE/GFE backend servers and Client workstations where vis|ability will be installed.

- Client Workstations
  - NET 4.8 or higher
- Backend Equipment
  - .NET 3.5 and .NET 4.8 or higher

Operating System Hardening

Activu offers hardening of Windows Operating Systems using Security Technical Implementation Guides (STIGs) as per the Defense Information Systems Agency (DISA). More information can be found at http://iase.disa.mil/stigs/Pages/index.aspx. For more information, please contact your Activu Implementation Team.

Group Policy

In those networks where Group Policy is deployed, Activu should have its own OU, or be otherwise excluded from GPs which may manage power, port exclusions, SNMP traffic, etc. Please discuss with System Engineer or assigned System Integrator the policies that may affect or interfere with the functionality of the Activu system.

See Appendix C for more information.

Data Recovery

By default, the vis|ability database is backed up automatically to the local system drive. Activu recommends targeting this database in your current backup routine.

Windows Updates

Clients should adhere to best practices when updating and patching vis|ability servers and workstations. Activu publishes a list of approved or flagged updates on our Client Support Portal

See Appendix C, Section 1a for more information.

Network Diagnosis

Clients should have the ability to evaluate common network metrics, configurations, and problems. Examples: broadcast storms, Spanning Tree configuration, routing loops, network congestion, etc.

Remote Access for Support

Activu requests that remote access to our system servers be provided through any means available from the customer. Remote Access can significantly improve the resolution of issues and provide remote configuration and training.

Activu offers a remote monitoring service as an add-on to our support and maintenance agreement. Please let us know if you would like more information on this.

Remote Management

iLo/iDRAC/OOM

Most Activu servers offer remote management via iLo or iDRAC, depending on how the system is engineered. Activu does not purchase any advanced or upgraded version of iLo or iDRAC unless otherwise requested prior to the purchase of the system. Activu also uses 3rd-party graphics cards in some servers which will disable RDP over iLo/iDRAC.

Remote Desktop Protocol

Please Reference Appendix C Section 2.g.

Virtual Machines

Server-based System Manager

Access to these is vital to our project implementation. In most cases, Activu will provide a “management” PC as part of the installation. This PC will be wired into the Activu VLAN you assign and needs the ability to remotely access the virtual machine acting as the vis|ability System Manager via your preferred remote access application.

Client-based content machines

vis|ability capture client software offers the ability to work in virtual environments, e.g. VMware vSphere. The use of virtual machines to host interactive websites or applications is encouraged as it provides ease of use for these source types.

User Authentication

Activu Authentication

Activu will store all groups and users inside our database

Windows Authentication via LDAP/LDAPS

Activu can import and authenticate groups and users via LDAP/LDAPS query

Requires that where our System Manager Service is running

Notifications from vis|ability System

vis|ability Mirrored systems

This can send notifications via email on mirror role change events, requiring the following to be provided:

- SMTP Address
- SMTP Port (SSL is supported)
- SMTP Username/Password

The Notification Service (NS)

NS is a component that communicates with an Activu-hosted, multi-tenant, AWS cloud-based server that sends notifications to customers via email and SMS text messages.

NS currently supports our Two Factor Authentication and Link notification features

Considerations for Web-facing features of Activu

Web-based features of vis|ability can listen on 443 or within the vis|ability default port range.

These components come default with self-signed certificates. Clients should be prepared to obtain security certificates for any of the web-based features that are in the scope of the project.

vis|ability Mobile

iOS is the only supported mobile operating system for the vis|ability mobility application.

Not available after version 6.5

vis|ability Web Portal and Web Client

Web Portal: Self-hosted with ASP.net web server listening on 443

Web Client: Self-hosted using technology WASM listening on 443

Recommendation: For external access to the web portal, a reverse proxy is recommended

https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/kestrel/when-to-use-a-reverse-proxy?view=aspnetcore-5.0

Considerations for Web-based Integrations with 3rd Parties

Activu currently has integrations with 3rd Party software that will require certain Activu software and/or equipment to communicate outside of your network

- v6.5
    - ServiceNow
    - Waze
    - Splunk
    - Email
    - Zoom
- v.6.6 (Q3 2023 release)
    - Teams

Appendix A: Bandwidth and Other Details for IP Video and Capture Client Decoding

This Appendix is valid for installations in Traffic Management Centers, Security Operations Centers or other centers that view IP video from a camera, encoder, NVR, or VMS.

vis|ability offers the capability to decode a large number of independent video streams simultaneously which, in some cases, corresponds to a large amount of network data. How much network utilization this represents varies with the resolution, frame rate, protocol, and transmission method, along with actual usage modeling.

Generally, to account for maximum usage, Activu recommends a 10Gb uplink if Activu is providing a network switch in the case of these installations. If Activu is not providing a network switch, the servers performing the rendering can be wired directly to a switch or switches that can provide sufficient bandwidth.

Activu also uses a 3rd party software known as CoreAVC to assist with optimizing decoding protentional by ensuring hardware acceleration is in use. CoreAVC is adjustable for both AMD and NVIDIA-based graphical hardware. Additional configuration documentation is available.

Appendix B: Activu Ports and Protocols

This appendix identifies ports for each vis|ability software module. These ports must be opened on any firewall for the respective service or application to function normally. It is recommended that you do not change these default ports.

Table A-1 lists the ports and protocols used by Activu services and/or applications.

Table A-1: vis|ability Ports

***Minimum ports required for Client to Server communication**

Protocol	Listening Port	Component	Service/App	Description
TCP/IP	***59081**	Nexus	Service	SSL/Encrypted
TCP/IP	59082	(Reserved)		
TCP/IP	59083	(Reserved)		
TCP/IP	59084	(Reserved)		
TCP/IP	59085	MUX	Service	RTSP Server port
TCP/IP	59086	MUX	Service	RTSP over HTTP port
TCP/IP	***59087**	MUX	Service	Receiver Bind port (ZeroMQ)
TCP/IP	***59088**	MUX	Service	Sender Bind port (ZeroMQ)
TCP/IP	59089	MAS (optional, def. 443)	Service	Mobility Server
TCP/IP	59090	Unreal (1935)	Service	Mobility - Streaming Server IN
TCP/IP	59091	Unreal (5119)	Service	Mobility - Streaming Server OUT
TCP/IP	***59092**	MUX	Service	HTTPS web service for LiveView
TCP/IP	59093	WebClientBlazorServer (optional, def. 443)	Service	HTTPS Web Server
TCP/IP	59094	Interface Server	Service	Interface for APIs/SDKs SSL
TCP/IP	59095	Interface Server	Service	Interface for APIs/SDKs
TCP/IP	59096	Link Integrator	Service	Link REST API
TCP/IP	59097	WebPortal (optional, def. 443)	Service	HTTPS web service
TCP/IP	59098	WebHookServer (optional, def. 443)	Service	HTTPS POST webhooks
TCP/IP	59099	(reserved)		

Appendix C: vis|ability Servers on a Domain

****NOTE – The Activu solution could be using different operating systems ranging from server class (Svr2016, 2019, 2022) to workstation-class (Win10 Pro, Win10 LTSC, Windows 11 Pro)**

Recommendations: Activu Servers/workstations are placed into their own Organizational Unit (OU) with the following items considered for the policy applying to this OU.

1. All Activu System servers
    1. No automatic Windows updates
        1. More on Windows updates:
            1. Patches (OS, AV, etc) for our Server and Workstation equipment should be applied once a month, on the weekend, at night, OR an agreed-upon maintenance window with the owner(s) of our system
2. All Display Nodes and Decoders Servers (if applicable)
    1. No screen savers
    2. No automatic OS lock
    3. No automatic log off
    4. Windows Firewall Policy – If required, appropriate exceptions need to be made
    5. Power Settings
        1. Set to Maximum or Ultimate performance levels
    6. *Typical Display Nodes and Decoders normally automatically log in but some domain policies prevent this. If auto-login is not allowed, anytime the server needs to be rebooted, someone will need to log into the server to allow the Activu application to start properly
    7. No Remote Desktop – Remote desktop can cause certain servers to be adversely affected by an RDP session. Console-level remote tools are recommended e.g. DameWare, VNC, etc.
        1. There are exceptions to this if Remote Desktop is the only option for remote access. Please ask your Activu Project Manager for more information.
    8. Local group policies - Our systems that come installed with GPUs have a local Administrative Template GPO in place to prevent any changes to the display layout. If this GPO is overridden with domain settings, the Display Node/Decoder will be at risk of not functioning as intended.
        1. Computer Configuration > Administrative Templates > Windows Components > Windows Update > Do not include drivers with Windows Updates = Enabled
        2. Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of devices using drivers that match these device setup classes = Enabled
3. All System Managers
    1. May have screen savers
    2. May auto lock
    3. May not automatically log off
        1. In the event of Activu System Managers running within a Microsoft Failover cluster, all components run as a Windows service and therefore can support auto log-off of a user.
            1. This also holds true for any control manager that requires this policy to be in place. If so, the ASM Service in Windows services will need to be set to use a local/domain account to run as.
        2. There are exceptions to this. Please ask your Activu Project Manager for more information.
    4. Windows Firewall Policy – If required, appropriate exceptions need to be made

4. Other Considerations
    1. Activu recommends two domain service accounts. One service account will require **local administrative privileges** to install, configure, maintain, and upgrade the software. For normal operation of Activu software outside of administrative functions, a domain service account with basic OS user rights will be sufficient.
        1. Note - in some cases, the basic user account might need file/folder privileges given to Activu software installed under C:\Activu
            1. Server 2016 and higher native domains support standalone Managed Service Accounts (sMSA) or group Managed Service Accounts (gMSA). Activu recommends the use of these when available as it provides automatic password management.
                1. REF: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

* if a service call is required to Activu support staff and a request to reboot the server is made, onsite staff will need to know the username and password of the domain service account in order to log back into the servers and in some cases physical access to servers will be required.

Appendix D: vis|ability component list

***For whitelisting considerations**

vis|ability component	**Executables**	**Entity Type**
Nexus	Visability.Nexus.exe	AB Admin
Display Node	visabilityDisplayNode.exe DisplayNodeViewer.exe ActivuWebContainer.exe CompositeWebViewer.exe AppWatcher.exe visabilitySpaceEngine.exe ActivuStandardViewer.exe VLCViewer.exe	DS TSENGINE
System Manager	visabilitySystemManager.exe	ASM
Multiplexer	visabilityMuxRouter.exe	MUXROUTER
Capture Client	visabilityCaptureClient.exe visabilityCaptureClientControlPanel.exe visabilityKeyboardMouseService.exe	AGENT AGENTSERVICE
Admin Client	visabilitySystemAdministrationClient.exe	ASMADMIN
Desktop Client	visabilityDesktopClient.exe	AP
Mobility Access Server	visabilityMobilityAccessServer.exe	
Interface Server	visabilityInterfaceService.exe	AIS
Base Client	visabilityBaseClient.exe	AB Client
Installation Manager	visabilityInstallationManager.exe	
Device Manager	visabilityDeviceManager.exe ADMModule.exe	ADM ADMModule

Decoder Server	visabilityDecoderServer.exe IP Camera viewers ActivuStandardViewer.exe VLCViewer.exe	
App Server	visabilityAppServer.exe visabilitySpaceEngine.exe	APPSERVER
Link Integrator	visabilityLinkIntegrator.exe	INTEGRATOR
Link Configurator	visabilityLinkConfigurator.exe	
Link Plugins	visabilitySNConnectorPlugin.exe visabilityEmailPluginService.exe visabilitySplunkPlugin.exe visabilityWebHookService.exe	
Mirroring Server	visabilityMirroringService.exe	MirroringServer
Web Client Server	Visability.Wasm.Server.exe	WasmServer
Notification Server	visabilityNotificationService.exe	NS
Web Portal	visabilityWebPortalService.exe	WEBPORTAL