

CenturyLink Technology Solutions Service Guide

Savvis Directory Services 1.0: Microsoft Active Directory

This CenturyLink Service Guide (“SG”) sets forth a description of Savvis Directory Services 1.0: Microsoft Active Directory (“Service”) offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Service Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

Version	Previous	Section Modified	Date
HOS-20141029-SG-DirectoryServices	HOS-20140911-SG-DirectoryServices	ALL	October 29, 2014

Table of Contents

Service Description	3
Tables and Appendices.....	5
Table 1.0 Roles and Responsibilities.....	5
Table 2.0 Active Directory Replication Traffic.....	6
Table 3.0 Active Directory Client Authentication Traffic	7
Table 4.0 Active Directory Trust Traffic	7
Table 5.0 Monitors for Microsoft Active Directory Service.....	8
Definitions:	9

Service Description

1. Standard Service Description: Savvis Directory Services 1.0: Microsoft Active Directory (AD) is a Managed Hosting service (the “Service”). The standard Service consists of the licensing, installation, configuration, administration, monitoring, maintenance and support for the software components listed in section 1.1. The Service Level Agreement (SLA) associated with this Service Guide is the “Managed Hosting Services SLA.”

1.1. Software Components: Customer selects the version, services and deployment scenario from the following sections.

1.1.1. Supported Versions:

- 1.1.1.1. Microsoft Active Directory 2003 R2
- 1.1.1.2. Microsoft Active Directory 2008
- 1.1.1.3. Microsoft Active Directory 2008 R2
- 1.1.1.4. Microsoft Active Directory 2012
- 1.1.1.5. Microsoft Active Directory 2012 R2

1.1.2. Supported Active Directory Services

- 1.1.2.1. Microsoft Active Directory, Directory Services
- 1.1.2.2. Active Directory Backups, Snapshots and Recycle Bin

1.1.3. Deployment Scenarios:

- 1.1.3.1. Stand-Alone Forest
- 1.1.3.2. Extended Domain
- 1.1.3.3. Child Domain

1.2. Licensing: Licensing is included in the CenturyLink provided Operating System subject to the Microsoft Service Provider Use Rights and License Agreement. All users of the service are subject to the terms and conditions of the referenced license agreement.

1.3. Installation: CenturyLink will perform installation tasks marked with an “X” in the CenturyLink column in Table 1.0 for the supported operating systems and hosting CenturyLink platforms listed below. Customer selects the operating system and platform at the time of purchase.

1.3.1. Supported Operating Systems:

- 1.3.1.1. Microsoft Windows Server 2003 R2
- 1.3.1.2. Microsoft Windows Server 2008
- 1.3.1.3. Microsoft Windows Server 2008 R2
- 1.3.1.4. Microsoft Windows Server 2012
- 1.3.1.5. Microsoft Windows Server 2012 R2

1.3.2. Supported Hosting Platforms:

- 1.3.2.1. CenturyLink Cloud
- 1.3.2.2. CenturyLink Dedicated Cloud
- 1.3.2.3. Intelligent Hosting

1.4. Configuration: CenturyLink will provide configuration tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.5. Administration: CenturyLink will provide administration tasks marked with an “X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.5.1. Security: CenturyLink utilizes NIST guidance for additional security standards when deploying Microsoft AD and will provide security policies for Microsoft AD to Customer upon request.

1.5.1.1. Active Directory Replication Traffic: Items are described in Table 2.0

1.5.1.2. Active Directory Client Authentication Traffic: Items are described in Table 3.0

- 1.5.1.3. **Active Directory Trust Traffic:** Items are described in Table 4.0
 - 1.5.2. **Access:** Customers are given administrative full control and Domain/Enterprise Admin rights to Managed Microsoft AD. CenturyLink will require an account within the domain with Domain, Enterprise and Schema Admin rights to perform a schema extension of both the Forest and Domain as described in Table 1.0. Any Outages directly caused by Customer's access will not be subject to SLA Service Credits.
 - 1.6. **Monitoring:** CenturyLink will provide administration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities CenturyLink will enable application level monitoring for each environment as they are created within the product configuration.
 - 1.6.1. **Production Environment Notification:** CenturyLink will retain primary notification and resolution responsibilities for all automated environment alerts in the production environment. The production environment is subject to SLA credits.
 - 1.6.2. **Non-Production Environment Notification:** A Customer technical contact will be engaged to perform primary resolution of incidents associated with a non-production level environment. The non-production environment is not subject to SLA credits
 - 1.6.3. **Monitored Values:** Table 5.0 describes the Monitors available for the Service.
 - 1.7. **Maintenance and Support:** CenturyLink will provide maintenance and support tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.
 - 1.7.1. **Patch Releases:** CenturyLink certifies, approves and delivers Microsoft Hotfixes for installation in a Customer environment. Customer must approve the installation by contacting CenturyLink support. Any Outages directly caused by Customer's failure to accept the implementation of a patch will not be subject to SLA Service Credits.
 - 1.7.2. **Change Management:** All changes to the CenturyLink managed applications; systems, network and facilities are subject to CenturyLink's change management process. This process is intended to confirm that work is reviewed for completeness (risk assessment, completed test procedure, metrics for measuring progress, back out procedure, etc.) and accuracy prior to scheduling and implementation.
 - 1.7.3. **Maintenance Windows:** All times listed under Maintenance Windows are local times and subject to change. CenturyLink will use commercially reasonable efforts to perform routine maintenance only during the Saturday or Sunday defined maintenance windows. See Definitions for additional information.
 - 1.7.4. **Support:** Support for the Service is provided through the project manager during installation, content migration and Customer validation. At the point of go-live the Service is passed from project management to CenturyLink Service Center for full 24x7 monitoring and management. The point of go-live is when Customer notifies CenturyLink project manager that the environment is ready to go-live.
- 2. **Customer Responsibilities:** Customer is responsible for all tasks with an "X" in the Customer column in Table 1.0 Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 1.0 may result in CenturyLink's inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer's failure.
 - 2.1. **Provide Contact:** Designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means a technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.
- 3. **Additional Services:** At Customer's option and expense Customer can choose to have CenturyLink complete one or more of the tasks in Table 1.0 with an "X" in the Customer column and/or the services listed below. The

items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work (“SOW”) or Service Order. Contact a sales representative for additional information.

- 3.1.1. **Minor Releases:** Minor Releases (see Definitions) require a new installation of the software binaries, which is not included in this Service. CenturyLink recommends that Customer purchase a new managed server (via a Service Order) and migrate data (defined in a SOW) as a best practice.
- 3.1.2. **Major Releases:** Major Releases (see Definitions) require a new installation of the software binaries, which is not included in this Service. CenturyLink recommends that Customer purchase a new managed server (via a Service Order) and migrate data (defined in a SOW) as a best practice.
- 3.1.3. **SSL Certificates:** SSL Certificates are small data files that digitally bind a cryptographic key to an organization’s details. When installed on a web server, it allows secure connections from a web server to a browser.

Tables and Appendices

Table 1.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer	
License	Procure SSL Certificate for LDAPs (if purchased)	X		
	Maintain Licensing and Support with Microsoft	X		
Installation*	Prepare Server for Active Directory (OS Specific Parameters)	X		
	Provide detailed requirements prior to physical build work		X	
	Install Microsoft AD and DNS services	X		
	Harden Microsoft AD to NIST and CenturyLink Standards	X		
	Install SSL Certificates for LDAPs	X		
	Install CenturyLink Monitoring	X		
	Perform Quality Assurance against Microsoft AD Installation/Hardening	X		
	Provide sign off that environment is ready to go-live		X	
	Configuration	Configure DNS Server services	X	
		Configure NTP Server services	X	
Configure DNS/NTP Client services on CenturyLink managed servers		X		
Configure DNS/NTP Client services on Customer managed servers			X	
Configure Sites & Services for CenturyLink Managed Sites		X		
Configure Trusts to CenturyLink Managed Domains		X		
Perform CenturyLink Supported Schema Extensions		X		
Configure Sites & Services for non-CenturyLink Managed Sites			X	
Configure Trusts to non-CenturyLink Managed Sites			X	
Perform non-CenturyLink Supported Schema Extensions			X	
Create/Modify CenturyLink standard Group Policies	X			

Activity	Task	CenturyLink	Customer
	Change Domain/Forest Function Level	X	
	Configure CenturyLink Monitoring	X	
	Install and configure CenturyLink Disk/Tape Backups (if purchased)	X	
	Data validation, User Acceptance Testing (UAT), Site Acceptance Testing (SAT)		X
Administration	Unlock User Accounts	X	
	Reset User Passwords	X	
	Disable Users	X	
	Application Log Monitoring	X	
	Update managed servers with all recommended security patches, service packs and hot-fixes upon customer request	X	
	Bulk Create Users/Groups (flat OU/Container)	X	
	Join CenturyLink managed servers to a CenturyLink managed Active Directory Domain/Forest	X	
	Join CenturyLink managed servers to a Customer managed Active Directory Domain/Forest		X
	Bulk Create Miscellaneous objects		X
	Create/Modify/Delete Users, Groups, OUs, Containers, DNS Records, Custom Group Policies, SPN Records and Miscellaneous objects		X
Migrate objects from an external environment		X	
Maintenance and Support	Backup Active Directory	X	
	Coordinate patching with Customer during maintenance hours	X	
	Perform an Authoritative Restore of Active Directory	X	
	Perform a Non-Authoritative Restore of Active Directory		X
	Perform an Object-Level Restore in Active Directory		X

*Installation is only supported on Domain Controllers with a single NIC

Table 2.0 – Active Directory Replication Traffic

Traffic	Protocol	Source Port	Destination Port
ICMP	ALL		
RPC Endpoint Mapper	TCP/UDP	1024-65535	135
RPC Dynamic Assignment * Default Windows 2003 R2 and earlier ** Default Windows 2008 and later	TCP/UDP	1024-65535	1024-65535* 49152-65535** 6000-6199
NetBIOS Name Service	TCP/UDP	1024-65535	137
NetBIOS Datagram Service	UPD	1024-65535	138
NetBIOS Session Service	TCP	1024-65535	139
SMB over IP	TCP/UDP	1024-65535	445
LDAP	TCP/UDP	1024-65535	389
LDAP over SSL	TCP	1024-65535	636

Traffic	Protocol	Source Port	Destination Port
Global Catalog LDAP	TCP	1024-65535	3268
Global Catalog LDAP over SSL	TCP	1024-65535	3269
Kerberos	TCP/UDP	1024-65535	88
DNS	TCP/UDP	1024-65535	53
NTP	UDP	123	123
SMTP	TCP	1024-65535	25

Table 3.0 – Active Directory Client Authentication Traffic

Traffic	Protocol	Source Port	Destination Port
ICMP	ALL		
RPC Endpoint Mapper	TCP/UDP	1024-65535	135
RPC Dynamic Assignment * Default Windows 2003 R2 and earlier ** Default Windows 2008 and later	TCP/UDP	1024-65535	1024-65535* 49152-65535** 6000-6199
SMB over IP	TCP/UDP	1024-65535	445
LDAP	TCP/UDP	1024-65535	389
LDAP over SSL	TCP	1024-65535	636
Global Catalog LDAP	TCP	1024-65535	3268
Global Catalog LDAP over SSL	TCP	1024-65535	3269
Kerberos	TCP/UDP	1024-65535	88
DNS	TCP/UDP	1024-65535	53
NTP	UDP	123	123

Table 4.0 Active Directory Trust Traffic

Traffic	Protocol	Source Port	Destination Port
ICMP	ALL		
RPC Endpoint Mapper	TCP/UDP	1024-65535	135
RPC Dynamic Assignment * Default Windows 2003 R2 and earlier ** Default Windows 2008 and later	TCP/UDP	1024-65535	1024-65535* 49152-65535** 6000-6199
SMB over IP	TCP/UDP	1024-65535	445
LDAP	TCP/UDP	1024-65535	389
LDAP over SSL	TCP	1024-65535	636
Global Catalog LDAP	TCP	1024-65535	3268
Global Catalog LDAP over SSL	TCP	1024-65535	3269
Kerberos	TCP/UDP	1024-65535	88
DNS	TCP/UDP	1024-65535	53

Traffic	Protocol	Source Port	Destination Port
NTP	UDP	123	123

Table 5.0 Monitors for Microsoft Active Directory Service

Monitors included in the standard Service at no additional charge

Monitor	Description	Frequency
Replication Queue	Alarms when the number of Active Directory synchronizations queued is above 1	5 Minutes
DNS Failures	Alarms when the number of Failed DNS Zone Transfer requests is above 1	5 Minutes
DNS CPU Usage	Alarms when the DNS service consumes more than 75% of the CPU	5 Minutes
DNS Memory Usage	Alarms when the DNS service consumes more than 35MB of memory	5 Minutes
FRS CPU Usage	Alarms when the FRS service consumes more than 80% of the CPU (2003 only)	5 Minutes
FRS Memory Usage	Alarms when the FRS service consumes more than 10MB of memory (2003 only)	5 Minutes
Active Directory CPU Usage	Alarms when Active Directory consumes more than 80% of the CPU	5 Minutes
Active Directory Memory Usage	Alarms when the DNS service consumes more than 60MB of memory	5 Minutes
LDAP Bind Time	Alarms when the Bind Time is over 600 milliseconds	5 Minutes
Time Offset	Alarms when the time offset between the local Domain Controller and the PDC is greater than 1 second	15 Minutes
Subnet Undefined	Alarms when a subnet is not defined for a site in Active Directory	Instantly
Connectivity	Alarms when a Domain Controller cannot be pinged, is not registered in DNS, cannot be reached via RPC or cannot be reached via LDAP	5 Minutes
Replication	Alarms when Replication is failing between Domain Controllers	15 Minutes
Topology	Alarms when the Active Directory Topology does not include all Domain Controllers	15 Minutes
Cut Off Servers	Alarms when a Replication Partner is offline	5 Minutes
Advertising	Alarms when a Domain Controller is unable to come online	5 Minutes
Role Holder Check	Alarms when a Domain Controller cannot locate a Role Holder	5 Minutes
Intersite Replication	Alarms when Intersite replication is failing	5 Minutes
FSMO connectivity	Alarms when a Domain Controller cannot reach a Role Holder	5 Minutes
Active Directory Services	Alarms when a core service for Active Directory is not running	5 Minutes
SYSVOL Access	Alarms when the SYSVOL share is unreachable	5 Minutes
Incoming/Outgoing Replication	Alarms when replication is failing	10 Minutes

Definitions:

Active Directory Client Authentication: Use Active Directory (AD) Client Certificate authentication to map client certificate information across many servers.

Active Directory Replication: The process by which the changes that are made to Active Directory objects on one domain controller are automatically synchronized with other domain controllers.

Active Directory Trust: An Active Directory trust is required to enable authentication between the Customer Forest (and any domains) and the Microsoft Managed Forest. The trust serves as the authentication pipeline that allows users in a domain to access Office 365 resources (such as a mailbox or SharePoint data) in a Microsoft Managed Forest.

Child Domain: The purpose of a Child Domain is to provide customers with single sign-on access to their CenturyLink Managed Hosting environment from their corporate infrastructure. Customer has the ability with this deployment to allow any end user in their existing corporate Active Directory Forest to access applications in the CenturyLink-managed Child Domain using their corporate identity. The extension of a Child Domain from the customer's existing corporate forest allows CenturyLink to manage Customer's managed services within CenturyLink, but CenturyLink employees do not have access outside of the Child Domain into Customer's corporate infrastructure. This deployment is most often used when the hosted infrastructure and or services with CenturyLink serve only the Customer's internal corporate users.

Clean Upgrade: Upgrade to a newer version of an operating system or application on a computer. In a clean upgrade of an OS, the hard disk is formatted and completely erased. In a clean upgrade of an application, the older version is uninstalled first.

Destination Port: Destination ports may be well-known ports for the major Internet applications, such as web and e-mail.

Domain Controller: A server within the Customer domain that is hosting the Active Directory domain.

Extended Domain: The purpose of an Extended Domain is to provide customers with single sign-on access to their CenturyLink Managed Hosting environment from their corporate infrastructure. Customer has the ability with this deployment to allow any end user in their existing corporate Active Directory Forest to access applications in the CenturyLink-managed Extended Domain using their corporate identity. The extension of a domain from the customer's existing corporate forest allows CenturyLink to manage Customer's managed services within CenturyLink, but CenturyLink employees do have access to the domain into Customer's corporate infrastructure, and this often drives customers to select the Child Domain implementation below. This deployment is most often used when the hosted infrastructure and or services with CenturyLink serve only the Customer's internal corporate users.

Hotfix: A hotfix or quick fix engineering update is a single cumulative package that includes information that is used to address a problem in a software product.

Maintenance Windows: A period of time designated in advance by CenturyLink, during which preventive maintenance that could cause disruption of service may be performed. Current Scheduled Maintenance windows are:

- Americas: Saturday 00:00AM to 5:00AM; Sunday 00:00AM to 5:00AM
- EMEA: Saturday 02:00AM to 6:00AM
- APAC (Except Japan): Saturday 21:00 (GMT) AM to Sunday 01(GMT)
- Japan: Sunday 04:00 (JST) to 8:00 (JST)

Major Release: Major Releases (X.y.z) are vehicles for delivering major and minor feature development and enhancements to existing features. They incorporate all applicable error corrections made in prior Major Releases, Minor Releases, and Patch Releases. Software Provider typically has one Major Release per year.

Microsoft Active Directory: Active Directory is a directory service implemented by Microsoft for Windows domain networks.

Minor Release: Minor Releases (x.Y.z) are vehicles for delivering minor feature developments, enhancements to existing features, and defect corrections. They incorporate all applicable error corrections made in prior Minor Releases, and Patch Releases. Minor Releases require a clean upgrade.

NIST: National Institute of Standards and Technology is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.

Non-Production Environment: A product is still being used theoretically. Users, typically engineers, look for bugs or design flaws.

Patch Release: Patch Releases (x.y.Z) are vehicles for delivering security fixes, feature developments, enhancements to existing features, and defect corrections. They incorporate all applicable error corrections made in prior Patch Releases.

Production Environment: A production environment can be thought of as a real-time setting where programs are run and hardware setups are installed and relied on for organization or commercial daily operations.

SLA Credit: Service Level Agreement Credits are refunds given by CenturyLink to a Customer if the Service falls below a contractually agreed service levels. See Section 1.0 for the SLA agreement associated with this Service

Software Provider: The third party that makes and sells software products described in section 1.0.

Software System: A software system is a system of intercommunicating components based on software forming part of a computer system (a combination of hardware and software). It "consists of a number of separate programs, configuration files, which are used to set up these programs, system documentation, which describes the structure of the system, and user documentation, which explains how to use the system".

Source Port: The source port is a next-available number assigned by TCP/IP to the client. This assigned number is how the network address translation method determines which user to send back the responses to

Stand Alone Forest The purpose of the Stand-Alone Forest is to provide customers with the ability to completely customize Active Directory for their needs within the CenturyLink environment, and provide single sign-on within the CenturyLink data centers. The Customer has to create an account for any user that needs access to CenturyLink's managed services with this deployment, and this deployment does not provide any integration to Customer's corporate infrastructure. This deployment is most often used when the hosted infrastructure and/or services with CenturyLink serve only Customer's customer base.

Statement of Work: A statement of work (SOW) is a formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client. The SOW usually includes detailed requirements and pricing, with standard regulatory and governance terms and conditions.

Upgrades: Upgrades mean a Major Release or Minor Release of the software.