OPTIMAL IdM
Identity & Access Management

101 Uses for a Virtual Directory

101 Uses for a Virtual Directory

What is a Virtual Directory?

Your corporate directory services and individual application identity pools are fragmented and sprawled throughout your enterprise. Each directory needs maintenance and probably a lot of clean up. Unfortunately, there is little time for such efforts. Consolidation of these fragmented identity services often takes many man-years of effort, costly consulting services, temporary software migration tools and the result is rarely the clean, pristine environment envisioned.

What if there were a way to 'join' all of these directory services, virtually, into a single view, without consolidation, without creating another database or pushing and pulling directory identity data back and forth across the network in a never-ending process of synchronization. What if you could use a single interface to maintain a single entity (logon) across all connected disparate directory services - including hundreds of Active Directory (A.D.) forests. Wouldn't be ideal to set, audit and maintain a single security policy for authentication (AuthN) and access, in real time, in one place? Further, what if you could view and manage all Active Directory forests in a single console - along with SQL identity tables, and thousands of legacy identity application pools of disconnected identity stores. This would require a virtual directory.

A virtual directory is a software layer that delivers a single access and management point for identity management applications and service platforms. The virtual directory functions independent of any single application. It acts as a firewall to applications and other directory services. It is a proxy layer. It accepts incoming requests and then (optionally) transforms those requests before they are presented to applications in other directory services. This functionality enables you to close numerous security gaps, and enables a multitude of new functionality and supportability scenarios.

VIS = VIRTUAL DIRECTORY

OPTIMAL IDM'S IMPLEMENTATION OF A VIRTUAL DIRECTORY IS CALLED "VIRTUAL IDENTITY SERVER", OR "VIS." IN THIS DOCUMENT, WE USE THE "VIS" ACRONYM INTERCHANABLY WITH THE TERM 'VIRTUAL DIRECTORY'

A New Way of Thinking

A Virtual Directory requires a new way of thinking about directory services. Many of us have spent decades architecting around the limitations of A.D. and unconnected directory service silos. For us, we think in terms of the Active Directory forest as a security and administration boundary. It's not unusual to find customers with a hundred or more A.D. forests. For many Microsoft directory architects, you were told to use the A.D. forest as a security boundary, so you correctly created multiple A.D. forests. Then the business told you to consolidate into a single forest because it was too hard to administer and secure multiple forests...or because of limitations in Office 365 or another business-critical application - and sometimes simply for other technical or political reasons.

A virtual directory has no such boundaries or limitations. All directory silos can be immediately accessed and managed in real time, yet secured down to the most granular attribute value level – far beyond what you could do in A.D. Further, our Virtual Directory requires no consolidation or cleanup.

Optimal IdM's virtual directory is called Virtual Identity Server, or "VIS." Our Virtual Directory is run in hundreds of customers world-wide. Some of the largest most recognizable customers on earth to some of the most secure government infrastructures.

Optimal IdM provides a heterogenous, vendor-agnostic identity platform. The functionality of our Virtual Directory (VIS) is not limited to a single vendor or directory or forest. The Virtual Directory is a piece of middleware that proxies traffic to/from the connected directories on the backend. VIS is managed through a familiar LDAP management tool. However, you need not use our management tool for the everyday tasks you currently do. You may choose to use our console periodically to create connections to backend directory services, create access policies, search all directories in one place, etc. Your junior-level administrators and help desk can still continue to perform admin functions as they do today.

VIS can run on-premises or in a fully managed instance in the Microsoft Azure or Amazon Cloud. Our Virtual Directory has an optional Federation component which

mmediately turns it into a full Federation Broker SSO solution. It is that very solution that is running at Fortune 1000 companies, governments and serves many of millions of authentications per month. For this whitepaper, we'll concentrate on the Virtual Directory (VIS) as an on-premises solution without the optional Federation services.

Often, we can deploy our Virtual Directory Server and have it up and running in less than 15 minutes.

Virtual Directory ≠ **MetaDirectory**

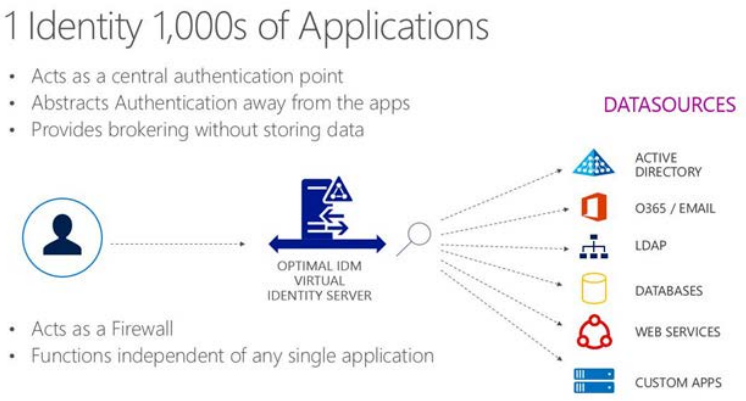
MetaDirectory versus a Virtual Directory

A virtual directory is not the same thing as a MetaDirectory service - e.g. Microsoft's MIM [formerly FIM, ILM, and MIIS], nor is it the same thing as an enterprise, "master" or "universal" directory.

A MetaDirectory is solely meant for syncing objects and not meant for LDAP enabled applications to connect to it - a MetaDirectory does not support/listen via the LDAP protocol. Conversely, a virtual directly is meant to enhance LDAP enabled applications.

Our virtual directory requires no synchronization between directories and therefore there is no data flow across the network, nor is there a need for database storage for directory identity data. Additionally, MetaDirectory services are plagued with orphaned objects as well as inconsistent and outdated data.

VIS uses real-time 'joins' cached at the proxy layer to connect data between disparate directory services and present them to apps and users as a single LDAP proxy.



101 Uses of our Virtual Directory

We'll start out with some of the highlights of the Virtual Directory, then drill deeper into scenarios and use cases. Lastly, because a few of the points seem redundant, though we assure you they aren't, we've include quite a few extra use cases to go well beyond the promised 101 uses of a virtual directory.

1. Return real-time data without storing it. Eliminate the need to synchronize data unnecessarily – VIS queries application data directly from its source - in real-time. In Optimal IdM's iteration of a virtual directory, there is no need to synchronize and create yet another repository database of identities and worry about keeping it updated.

2. Transform, merge and map data from multiple LDAP directories to a virtual name or namespace (e.g. Lotus Notes and Exchange Users could login as single_user_name@singlenamespace.com

3. Emulate another directory – Emulate a Sun LDAP while sourcing data from A.D. LDS

4. Emulate a Single Directory Store – VIS can mimic a single identity store (e.g. a single A.D. forest) to an admin/user/application - all without synchronization

5. Use our VIS Server's custom API to embed the full power/features of the virtual directory INTO your application - no need for separate server or proxy server

6. Setup Security Policies based on the network traffic flowing between client & server/application

7. Simple Password Synch – when you update the password through the virtual directory layer, we can then pass it on to the disparate backend directory

8. Add Multi-factor AuthN (MFA) to any app behind the proxy - at the LDAP layer without changing the application in any way

9. Master Directory - although rarely recommended, we can turn on optional synchronization our Virtual Directory (VIS) to be used as an enterprise cache or sometimes referred to as a 'Master' or 'Universal' Directory. [Note: We believe this option of additional storage of I.D.s presents more risk than reward for most customers].

10. Add SSO to any app Federated behind the Virtual Directory with our optional Federation component

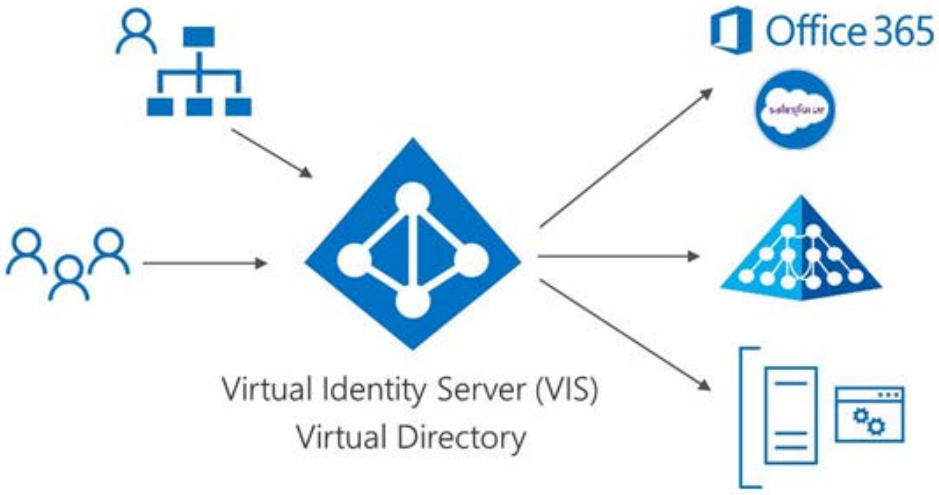
11. Enable immediate off-boarding (when a user leaves or is fired) scenarios at the proxy level, immediately preventing all AuthN requests

Mergers, Acquisitions and Divestiture Tools

12. Merger and Acquisition Tool – provide immediate, real-time joins of all directories across any boundary - even across the internet. (more details below)

13. Divestiture tool – use VIS to immediately give split forest views of identities and/or create new ones on-the-fly

14. On-the-fly Migration of the data to new data store - e.g. Authenticate to Sun, if successful create data in new LDAP, set user password, and flag as moved



Multiple Active Directory Forest Support

The Active Directory Forest boundary is not a boundary for our virtual directory. We can connect to hundreds (or even thousands) of A.D. forests and provide a single, unified view of your A.D. environment to search, manage and set policy. Do all of this without the need to create, manage, maintain or troubleshoot cross-forest trusts!

15. View hundreds of Active Directory (A.D.) forests in our single console

16. Authenticate across multiple A.D. forests - without A.D. trusts

17. Manage hundreds of A.D. forest - without A.D. trusts

18. Chain LDAP requests (from users or applications) to different forests

19. In a multi-forest environment, project a single A.D. forest from the VIS layer to LDAP apps that can only support one forest

20. Provide cross-forest group membership with no trusts needed between A.D. forests

21. Join thousands of different directories (even SQL identity tables) into our single interface

22. Translate Foreign Security Principals (SIDs) into Distinguished Names (DN) - e.g. instead of seeing a SID from another forest/domain, VIS can translate that to a friendly name CN=MarkJones,OU=Sales,DC=CompanyName,DC=COM

23. Translate binary directory data through VIS with the friendly value - e.g. translate the last logon time to a friendly value

24. Aid in domain/forest consolidation - change your A.D. structure while using VIS to project the 'old' A.D. structure to users (or applications) - applications will still 'see' the old structure and just work

> *"**Identity is the new security boundary.**" – Mark Simos*

Search, Profile & Secure User Accounts

Optimal IdM's Virtual Server provides a single pane of glass for identity management across all connected directories - including all A.D. forests.

25. Identify users that haven't logged into Active Directory in 'X' amount of days

26. Identify users that haven't changed their passwords

27. Identify users that are vulnerable for attack by attribute or condition you set

28. Use VIS to correlate Identities and discover orphaned accounts/rogue identity

29. Create workflow to place all disabled users from each A.D. forest into an OU created in each forest to contain them. Then place policy against those disabled accounts - either at the VIS proxy layer or within their forests.

30. Identify all disabled users across all A.D. forests and put them into a virtual OU or virtual group in VIS. [Note: Virtual OUs and virtual groups only show up in the VIS Management console, therefore your neither your A.D. forest admins, Enterprise admins, domain admins, OU admins nor your helpdesk will not see the virtual containers]

31. Create Policy against the virtual OUs and/or virtual groups in the example above

Secure LDAP Proxy & Directory Firewall

Our Virtual Directory serves as an ideal secure LDAP Proxy and Firewall. An LDAP Proxy server for your directory services can provide a host of benefits - including centralized Identity Policy enforcement, management, logging and auditing.

Authentication is abstracted away from the applications. Administration policies and functions are performed independent of application directories; therefore, at the VIS layer you are never held hostage to any individual application owner. VIS support centralized identity and security polices for a granular delegated administration model.

LDAP traffic is often unsecured which makes it possible for others to intercept and read traffic using network-monitoring software (and malware) between clients and servers. By default, a user LDAP object can view/read the entire directory - this applies to your Active Directory infrastructure and domain controllers. In fact, in Active Directory privileged group members are discoverable and readable by the "Authenticated Users" group, allowing any user to view the entire directory - including secret and renamed Admin users.

32. Deploy the LDAP proxy/firewall, connect to A.D. and start filtering connections in about 10 minutes - no joke

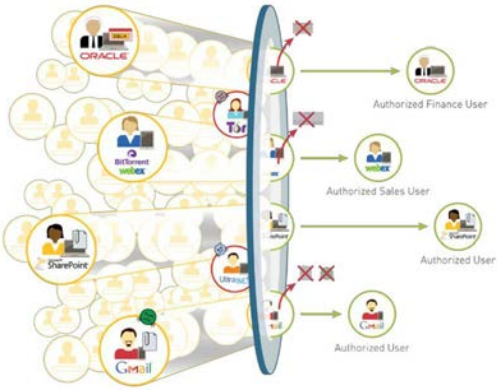
33. Cloud App Firewall - use to limit what cloud services (apps) coming into A.D. can see and have access to - e.g. a specific OU

34. On-Prem LDAP Firewall - the VIS instance can hide/filter on-premise directory requests to only the granular part of your directory service they need

35. Hybrid Firewall – both cloud and onpremise at the same time

36. Hybrid AuthN Solution – we can use the Virtual Directory to make the decision WHERE a user goes to AuthN - to the cloud or on-premise

37. Quick Solution for your DMZ for AuthN/AuthZ applied to your internal A.D. - for customers who have A.D. in their DMZ, we can control which forest/domain/OU or SQL table a lookup is confined to



38. Deny Access to any/all directory data from untrusted networks via the VIS proxy

39. Provide compliancy within country or regional regulatory boundaries by restricting READ rights to directory data from only certain IP ranges or geo-location attributes

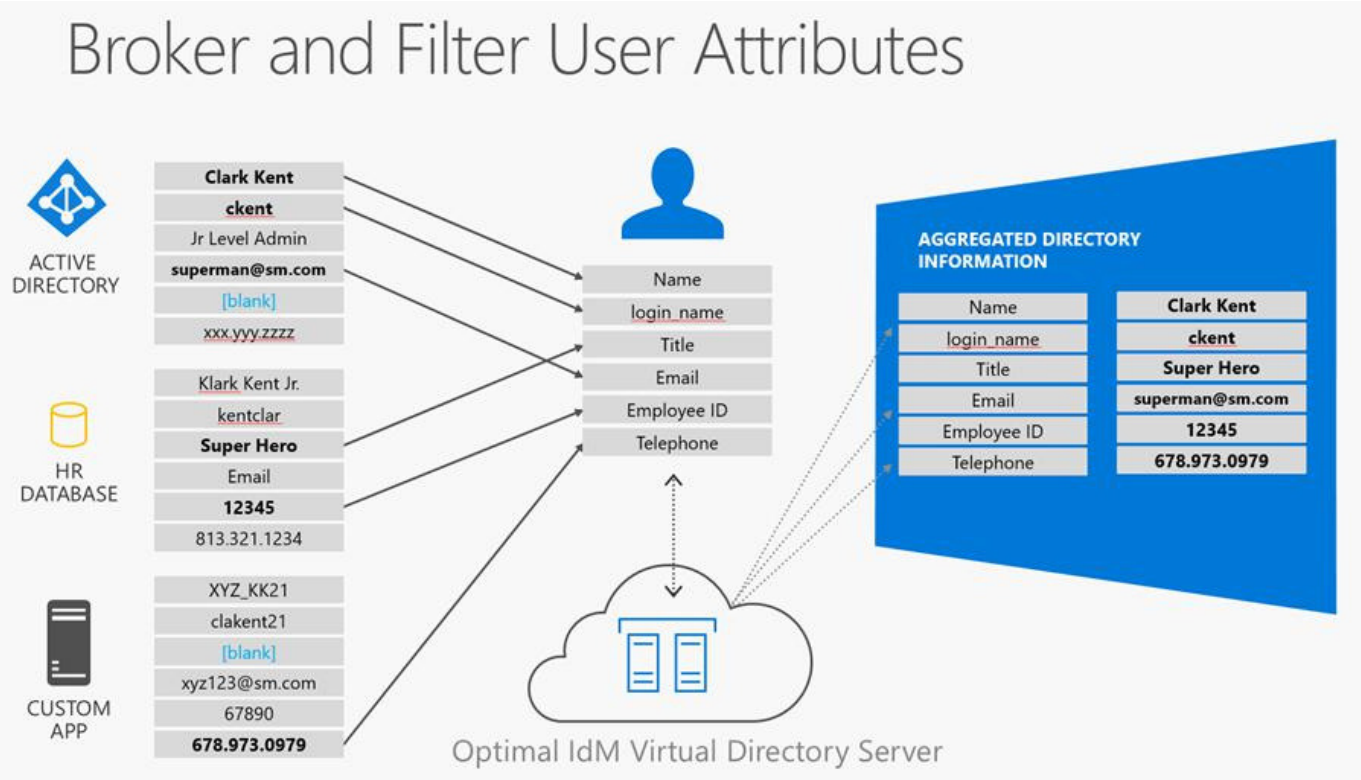
40. Refuse logon services to a user based on a central admin policy and not reliant on individual application owner at the VIS proxy layer; therefore, preventing further AuthN requests to be channeled to other directories

41. Provide Denial of Service Detection/Notification (Log/email, etc.) - VIS is the proxy layer that is the first point of authentication (AuthN); therefore, VIS can see, report and run conditional rules against attacks

42. Manage directory security/policy in a single place, at the proxy (VIS) layer, yet leverage for cloud applications, on-premise applications, SQL identity tables, web applications and LDAP

43. We can enforce secure binds to VIS.

44.Allow different rights/access to data (i.e. update or read only) on an application by application basis



Adaptive Authentication (or Adaptive Access Control)

Adaptive AuthN allows for AuthN decisions to be based off risk calculations. This can be a simple rejection of a legitimate user login rejected solely based on where (e.g. the network or IP range) it is coming. Or a risk decision from multiple complex calculations.

45. Allow different rights/access to data (i.e. update or read only) based on IP Address
46. Whitelist or Blacklist on only specific IP Addresses or ranges
47. Make AuthN decisions based on header variables
48. Make AutnN decisions based on the user agent (browser)
49. Make AuthN decisions based on date/time
50. Make AuthN decisions based on geo-location
51. Make AuthN decisions based on extensible temporary directory data held only within the Virtual Directory (hidden from A.D. and other directories)
52. Make AuthN decisions based on calculated directory information - e.g. only if a user is a part of XYZ group and is from XYZ A.D. Forest
53. Make real-time AuthN decisions based on a combination of any/all of the above

Extend Active Directory in New Ways

Do things at the Virtual Directory layer that are impossible in Active Directory. The Optimal IdM Federated Services product also includes a pluggable attribute store module that can surface attribute/claims from many different stores including nearly every LDAP on the market (ADAM, AD-LDS, Sun, Oracle, eDirectory, Open LDAP, OpenDS, etc.) as well as most databases (SQL, Oracle, DB2, etc.).

54. Populate all managers and their direct reports across untrusted forests
55. Provide a delegated administration model within the virtual directory that doesn't show up in the A.D. forests
56. Provide a delegated administration model based off real-time, dynamic, calculated directory identity values
57. Change your A.D. structure without impacting applications - no matter what changes you make to your A.D. structure, VIS can project the 'old' (or different) structure to users or apps
58. Use as a tool for redesigning your A.D. infrastructure – you can design and implement a new A.D. structure and use VIS to project the way the 'old'

forest(s) looked to provide compatibility to legacy apps tied to the old A.D. structure
59. Use VIS to provide printers a single unified look up of data
60. Create new virtual OU's in the Virtual Directory layer for administration based on any directory data
61. Extend ADFS with an attribute store to VIS - source claims from any data source beyond A.D. and SQL to eDirectory, for example.
62. Delegated Administration granularly down to a single container/user
63. Limit helpdesk access and display only to specific user attributes
64. Allow A.D. Federation Services to authenticate users beyond Active Directory - users can exist anywhere

Active Directory Schema Emulation

Another impressive feature of VIS is its ability to emulate schema extensions to Active Directory Forests. Many Microsoft and third-party applications that integrate with A.D. require permanent A.D. schema extensions - like Microsoft Exchange or Cisco's WebEx.

Admins are hesitant to make permanent changes to the Active Directory schema. Further, schema extensions to A.D. need to be made, and kept up-to-date, in all of your A.D. forests. You can use the Virtual Directory (VIS) to store and emulate those schema extensions to the apps that need them - without touching your A.D. forests. Since VIS is the first connection point of your users and apps, VIS can project those schema extensions into applications that are looking for them.

65. Emulate A.D. schema extensions for 3rd party apps yet allow them to work
66. Use the Virtual Directory layer to aggregate schema across all Active Directory Forests in a presentation layer - our LDAP viewer

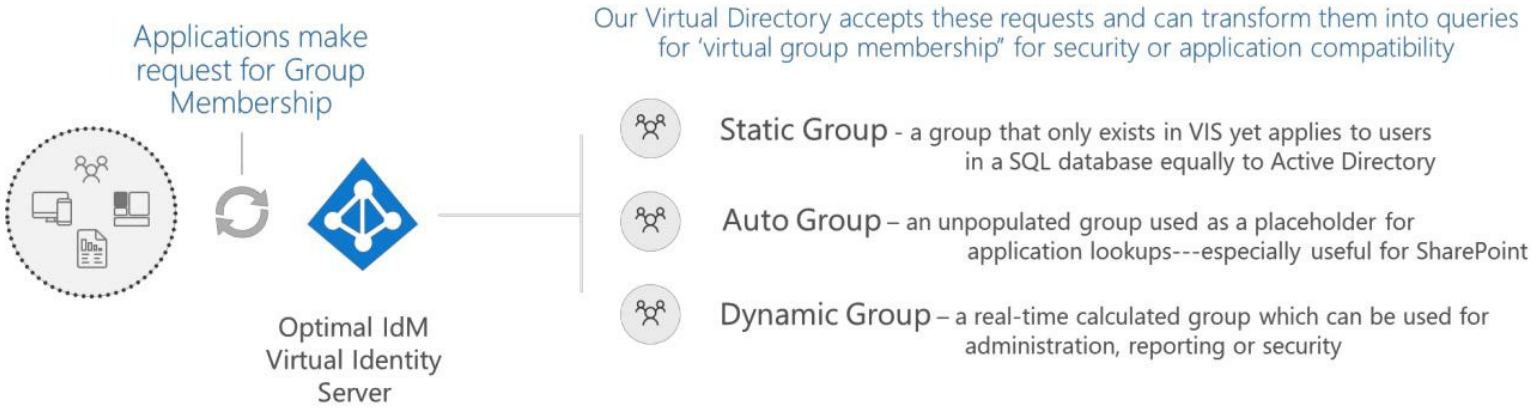
67. Build your own schema - our Virtual Identity Server allows you to build your own schema within our server and project it out (emulate it) to connected directories or applications that could consume it. Actually, each app could have its own schema.

Extend Active Directory in New Ways

68. We provide an API directly into the Virtual Directory for customers who prefer to hook directly into the Virtual Directory.

Extend & Expand The Use of Groups and Roles

VIS supports the ability to create three (3) new types of groups that Active Directory doesn't (and can't) store and support. These groups are **Dynamic Groups, Static Groups** and **Auto Groups**. Each has a distinctive use case and all can be used across forests or other directory boundaries.



Dynamic Groups, Static Groups & Auto Groups

Dynamic Groups are created by creating conditions within our LDAP interface. These conditions act as filters to create a group of users that exist only in the Virtual Directory (VIS). When the condition/rule for the group changes, the dynamic group(s) are immediately updated. These groups are available at the LDAP proxy layer and not projected into Active Directory

69. Create a Dynamic Group for all users across forests without trusts - e.g. create a "marketing group" from users across hundreds of Active Directory Forests in real-time
70. Create a Dynamic Group for Reporting – create a dynamic group based on conditions for reporting - e.g. create a dynamic group consisting of all users who geographically exist within XYZ namespace and in a given set of IP subnets
71. Create a Dynamic Group for Application Compatibility
72. Create a Dynamic Group for Security– the group is calculated and populated in our VIS LDAP viewer. (if NOT a member of "Executive Managers" group in any forest; then restrict them from seeing XYZ application
73. Create a Dynamic Group to (optionally) write back groups into A.D. and keep them updated
74. Auto Group = An Auto Group is for applications, like SharePoint, needs to check that a user is a part of a given group, but doesn't need to enumerate the

group memberships. This is great for cross-forest needs - again, A.D. trusts are not needed.
75. Use Virtual Static Groups - Groups across multiple identity data repositories - e.g. make a group that only exists in VIS that applies to user in a SQL database that equally apply to Active Directory users
76. Create VIS virtual groups to reduce the number of A.D. groups that need to be managed
77. Create Virtual Group Objects based on any A.D. attribute(s)
78. Create Virtual Group Objects based on any condition - create a dynamic group of all user objects across all forests that are disabled.
79. De-reference nested A.D. groups - which A.D. doesn't support
80. Provide a blended view of group membership across two different types of LDAP's - (e.g. Active Directory and Sun directory)
81. Allow the memberof attribute to be updatable

Azure A.D. Office 365 & SharePoint Support

82. Deploy Office 365 immediately without consolidation of existing A.D. forests and domains
83. Deploy Office 365 immediately without the need to synchronize your identities to the cloud
84. Enable Office 365 to have users in identity stores other than in only A.D. - e.g. a SQL table of users
85. Support for customers with non-routable domains for a User Principal Name (UPN) such a JoeUser@domain.local
86. Support for customers with multiple UPN suffixes - with no data changes required in Active Directory
87. Provide a unified GAL from multiple A.D. forests - without synchronization or trusts
88. Provide a unified GAL from other email systems such as Lotus Notes
89. AuthN Solution for SharePoint – VIS supports SSO for multiple A.D. forests into SharePoint 90. Provide a SharePoint profile import (push) of identity data in any directory store - not just in A.D.

Vijay Kumar, Senior Technical Product Manager states, "We are pleased that federation between VIS for Office 365 and Microsoft Office 365 has been verified and found to be interoperable so that our customers can take advantage of this solution".

SQL Server

Similar to other applications, and databases, Microsoft SQL Server can integrate with A.D. or have its own AuthN. SQL Server AuthN logins are created in the local SQL database store - independent from Active Directory. Our Virtual Directory, VIS, can read the SQL fields and translate them to/from A.D. or other directory identity stores. Again, all of this is done virtually - without synchronization to other directories.

92. Provide SSO to SQL Server AuthN through the Virtual Directory

93. Read data from SQL and present as LDAP data Allow SQL identity data to project into the proxy layer for use/reference by any/all applications

94. Manage and/or create the dynamic/auto-groups for apps that use their local SQL identity store

95. Use SQL queries against the virtual directory (VIS) to return LDAP data

96. Translate LDAP Updates into SQL updates in database - e.g. update a costcenter attribute in VIS and have it write the update to where the stored SQL directory data exists

97. Present multi-row SQL as multi-valued directory service attributes - if you define a role in SQL, it can be projected by the Virtual Directory as a multivalued object in A.D.

Fix, Secure & Extend Applications

VIS is an application enablement tool - allowing you to do things that you can't natively do in the application; or is too complicated; or isn't surfaced in the native GUI toolset of the application and/or something you would need more licensing to do.

VIS is also a central authentication point for all application which can be geo-distributed for high availability.

Since the Virtual Directory (VIS) is the proxy layer, we can transform directory 'calls' into nearly anything we want at the Virtual Directory layer, then present those transformed requests to backend directory services - for application compatibility, security, auditing and more.

98. Block anonymous searches through VIS to directories that would otherwise allow it
99. Enable anonymous searches to directories that don't allow it
100. As backend systems fail, VIS provides the failover mechanisms automatically at the VIS proxy layer. All applications now can have built-in failover.
101. Provide a way to notify administrators if a back-end system (connected directory store/service) goes down – we'll know immediately at the VIS layer
102. Fix applications that don't do LDAP paging of multi-valued attributes, our Virtual Directory will do that at the proxy level so the apps will just "work"
103. Provide different paging settings for different applications (and different from A.D.) - we can transform an LDAP paging 'call' at the Virtual Directory layer
104. All applications now have built-in connection pooling to A.D. which increases performance and reliability significantly
105. The VIS reporting logs gives you the ability to do a "replay" of exactly what an application is doing/did at the LDAP layer
106. Force applications to only use SSL - we can disable non-SSL connections at the proxy level and force applications to use our SSL connection
107. Provide an easier way for administrators to control which specific Active Directory servers applications can use - e.g. most apps have bad logic
108. Our VIS server can enumerate a 'virtual GUID domain or forest' to applications that are hard coded to a GUID, domain, or forest without

changing the application – ideal for times when you are going to decommission A.D. domains and forests

109. Map multiple attributes to the same attribute name - you can present SN (surname) and map it as LastName to an app that only understands it in that form 110. Format a phone number differently based on the user's or application's IP address - e.g. we can add the country code if it doesn't exist

111. Provide a flatten view of all objects from multiple OU's into a virtual single OU structure for administrative management

112. Bridge Apps that only support users in a single OU

Transform LDAP & Directory Functions Based on Conditions

113. Provide a "hook" to run a custom function via a pre/post on every LDAP operation (e.g. workflow)

114. Route Authentications from the VIS proxy based on conditional rules - e.g. only allow AuthN requests to a specific app/service based on geography or time of day (just about any condition you can make from directory data)

115. Route searches from VIS based on conditional rules - e.g. route searches intended for a 'secret' application to a SQL store, for instance

116. Block (e.g. whitelist, blacklist) LDAP and directory searches to apps through the VIS proxy

117. Route anything based on your rules...

118. Authenticate applications on multiple attributes - with no change to the application (userid, samaccountname, email, UPN, etc.)

119. Create "computed attributes" based on a rule (e.g. "IF" user belongs to x-y-z then do some time of custom action)

120. Extend LDAP to add additional commands such as NOW (we have filtering based on Key Words) - Show me all users created NOW minus 10 days and return the value

Use to Backend Directories In A Single Place

121. Remove attributes normally returned in an LDAP search - even if the attribute is requested by the application

122. Aggregate multiple A.D. partitions into a single A.D. partition – provide a unified OR separate view of the A.D. partitions - e.g. domain, schema, etc.
123. Present an app by app view based on the application and a security group or other rules (we can filter out views of the directories
124. Exclude certain searchbases/ou's from all applications
125. Provide the "Principle of least privilege" by only providing the applications ONLY the data they need
126. Provide Denial of Service Detection/Notification (Log/email, etc.)
127. Prevent users, admins and applications from searching on encrypted attributes
128. Alter data returned in search by an application or user
129. Encrypt data and certain attributes before presenting it back to the user or app - e.g. SSN
130. Provide Denial of Service Prevention (Virtually lock the account at the virtual directory)
131. Secure all back-end systems from applications on a granular attribute by attribute basis, if needed

Logging, Auditing & Reporting

132. VIS provides complete and consistent auditing across all applications with no changes to the application
133. A Virtual Directory, like VIS, can provide a real-time reporting view across the enterprise – the VIS server is a proxy and therefore a single point of AuthN logging and reporting
134. VIS enables real-time reporting of all accounts set with insecure values in the attribute – e.g. like PwdNeverExpires
135. VIS allows you to have a single place to search against any defined directory attribute or value from all connected backend directories
136. Use audit data to provide "charge backs" to business units
137. Provide a mechanism for applications to know where the data came from (attribute by attribute)
138. Hook in monitoring tools to notify administrators is different systems are too slow (i.e. searches taking too long)
139. Use our PowerShell commandlets that have the virtual directory embedded into them to get and return data from multiple sources

End-User Self-Service Functions

140. Provide end-user self-service functionality to register a new account
141. Provide end-user self-service functionality to reset password (via a simple webpage)
142. Provide end-user self-service for group management (add, create, join, leave, or renew group object membership)

Add-Ons

Our virtual directory can be extended in numerous ways. We offer an optional Federation Broker on top of it supporting thousands of applications, including Office 365, MFA enablement, workflow, end-user self-service and more. Additionally, from customer feedback Optimal IdM offers a fully managed IDaaS service which is the only one of its kind on the market.

143. VIS provides a building block for Optimal IdM to build a Federation Broker on top and extend SSO support to thousands of other applications. Please see our additional documentation on our award winning SSO Federation Broker and MFA Services.
144. Fully managed IDaaS service. Several of our largest customers' feedback has been to make our Virtual Directory Solution with Federation, Office 365 and SharePoint integration along with our award-winning MFA solution available as a fully managed IDaaS service in the cloud. We do so in a private, fully siloed, single tenant, private cloud - as an extension of your datacenter. We provide a web portal and only surface the administrative tools and user self-service functions that you request. All patching, updating, networking, storage, backups, high availability, reporting and monitoring is done by our experts. Additionally, we provide visualizations and graphic reporting done through Azure Reporting Services – which, of course, integrate with Power B.I. and Microsoft Excel.

Did You Know?

- Unlike other enterprise identity management software, the Virtual Identity Server can be installed and leveraged completely in a production environment in about an hour?
- In an article, Gartner lists 6 quick wins in Identity Management 3 of the 6 involved using a virtual directory?
  https://www.gartner.com/newsroom/id/1293115

  - **Optimal IdM's Virtual Identity Server**
  - Heterogenous, vendor-agnostic, multi-platform support
  - Standards compliant, yet customizable- we support all apps
  - No vendor lock-in
  - No synchronization or storage of IDs
  - No cleanup of existing disparate directory services needed
  - Highly familiar LDAP management interface
  - Deployed in hours, not weeks or months
  - No per application management
  - No redevelopment of applications
  - No repackaging and redeploying applications
  - No Software Agents deployed on Domain Controllers or any backend directory services

Recent Accolades

Optimal IdM has been positioned by Gartner, Inc. in the Niche Players quadrant of the Magic Quadrant for Access Management, Worldwide in 2017 and 2018, and featured on the Best Identity Management Solutions list of 2017 and 2018 by PC Magazine. Optimal IdM has also been named "Best Multifactor Authentication Solution" in the Government Security News (GSN) Homeland Security Awards (HSA) Program under the Cyber Security Products and Solutions category and named a Leader in KuppingerCole Leadership Compass Identity as a Service: Single Sign-On to the Cloud Report.