VMS Authentication Module

The VMS Authentication Module Solution

The VMS Authentication Module (VAM) provides controlled access to both user-written applications and the OpenVMS system overall using LDAP, RADIUS or the local VMS User Authentication File (UAF). It can be incorporated into an OpenVMS-based platform in three ways:

- Via an API that can be incorporated into an application to control access to that application
- On a system-wide basis by using the OpenVMS ACME system on OpenVMS V8 and higher on Alpha and Integrity platforms
- On a system-wide basis via use of the LGI callouts for OpenVMS `LOGINOUT.EXE`.

Easy to Install and Operate

Process Software's VAM product integrates cleanly into the OpenVMS environment. It supports the MultiNet and TCPware TCP/IP stacks and HP TCP/IP Services.

VAM is easy to install using the `VMSINSTAL` installation procedure. It takes less than five minutes to configure. The system administrator can control VAM by editing the configuration file.

Highly Configurable

VAM's configuration file is robust and can be customized to meet an organization's specific security requirements.

For example:

- Rightslist identifiers may be granted to specific users to determine if they should use VAM's authentication methods.
- All users may be required to use specific VAM authentication methods.
- Multiple authentication methods (e.g., first attempt LDAP then RADIUS) may be specified.
- Multiple LDAP searches and servers may be specified.

Configuration Support

VAM supports Alpha, and Integrity systems running various versions of OpenVMS. When each node in an OpenVMS cluster shares a common system disk, the cluster needs to store just one copy of most VAM files. Only a few system-specific configuration files are required on each machine that runs the software.

API Support

An application programming interface (API) is provided to allow VAM to be incorporated into existing user applications. The heart of the API is the `VMSAuthenticate` function call, where the calling program supplies (as required) the

© Process Software Corporation and/or its affiliates. All rights reserved.

username and password to be authenticated, the type of authentication (LDAP, RADIUS, or LOCALUAF), and pointers to user-written callbacks in the user program. These callbacks are used by VAM to communicate with the user (e.g., to prompt for passwords or to provide informational messages).

The Core Features of the VMS Authentication Module…

VMS Authentication Module enables remote systems administrators, telecommuters, and other users to access corporate networks without revealing passwords and confidential data to potential eavesdroppers.

- Supports LDAP authentication via an API, as a VMS ACME agent, and as a VMS LOGINOUT callout module.
- Provides additional access controls through the use of the VMS User Authorization File via an API.
- Supports the widely-used LDAP V3 protocol as found in, for example, Microsoft Active Directory and OpenLDAP.
- Allows fetching of user-defined attributes from an LDAP directory for a successfully-authorized LDAP user.
- Allows multiple searches of multiple LDAP servers.
- Includes LDAP client/server security options by supporting both plain-text (LDAP) and encrypted (LDAPS) transactions.
- Supports RADIUS authentication via an API, as a VMS ACME agent, and as a VMS LOGINOUT callout module.
- SSH single sign-on access using Process Software's MultiNet, TCPware and SSH for OpenVMS products.
- Provides many-to-one mappings of LDAP and RADIUS usernames to a single VMS username.

VMS LOGINOUT Callout Support

VAM provides a callout module used to implement LDAP and RADIUS authentication using the standard VMS LOGINOUT mechanism. It may be configured so that if a VAM login can't be completed for any reason other than an invalid username or password (for, example, in the case of a network outage that prevents communication with an LDAP or RADIUS server), the normal VMS SYSUAF will be used to validate the user.

VMS ACME Support

VAM provides LDAP and RADIUS agents for the VMS ACME (Authentication and Credential Management Extension) subsystem for OpenVMS V8 and higher on Alpha and Integrity platforms.

LDAP Support

VAM provides a client for LDAPv3 servers on various platforms. Examples of supported servers are Microsoft Active Directory and OpenLDAP from the OpenLDAP Foundation.

This client may be used in the form of an API that is incorporated into an application, as a VMS ACME agent, or as a callout module for the VMS LOGINOUT mechanism.

Transactions with LDAP servers may be performed using unencrypted clear-text (the default), or the transactions may be encrypted using certificates. The VAM configuration file is used to specify if transactions are encrypted (LDAPS) or not (LDAP).

To provide maximum flexibility, multiple searches may be specified for any supported server, and multiple servers may be searched. The servers and searches on those servers are specified in the VAM configuration file by the system manager. Searches are first conducted using either a specified Distinguished Name and password or anonymously (where supported by the server). In addition, all LDAP usernames may be mapped to a single VMS username on the client system.

© Process Software Corporation and/or its affiliates. All rights reserved.

When a user is successfully authenticated via an LDAP directory, attributes (as specified in the configuration file) may be returned. If using the API, these attributes are returned as a list of attribute/value tuples. If using the VMS ACME system, the attributes are set as logical names in the process's process logical name table. If using the LOGINOUT callouts, the attributes are set as logical names in the process's job logical name table.

If using the LOGINOUT callouts and upon successful authentication, the last login date and time and the user's password are updated in the VMS UAF file, to ensure the information is as synchronized when possible. This behavior may be overridden by the `LDAP_NO_PASSWORD_SYNC` keyword in the configuration file.

RADIUS Support

VAM provides a client for RADIUS server systems on various platforms. An example of this would be a server running the FreeRADIUS server.

This client may be used in the form of an API that is incorporated into an application, or as a callout module for the VMS LOGINOUT mechanism.

Transactions with RADIUS servers are performed using unencrypted clear-text data, but with the password encrypted using MD5 encryption.

In addition, all RADIUS usernames may be mapped to a single VMS username on the client system.

If using the LOGINOUT callouts and upon successful authentication, the last login date and time and the user's password are updated in the VMS UAF file, to ensure the information is synchronized when possible. This behavior may be overridden by the `RADIUSNOPASSWORDSYNC` keyword in the configuration file.

VMS Local User Authorization File Support

The local User Authorization file (UAF) may be used within the API to provide authentication for an application.

© Process Software Corporation and/or its affiliates. All rights reserved.

Services, Documentation, and Ordering Information

Technical Services

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, training, software maintenance, support, online resources, and 24-hour support - in short, everything you need to keep your Process Software products and your network operating at peak efficiency.

Consulting

A comprehensive suite of programs is available on a host of topics, including VMS Authentication Module installation and configuration, network security, troubleshooting, and others.

Hot Line Support

Networking experts are available by telephone and e-mail. Optional 24-hour support is also available.

Updates

All maintenance customers with current service contracts receive automatic software and documentation updates of major releases.

Training

A wide range of educational services can be provided at your site, at regional training locations throughout North America, or at our own training facility in Framingham, MA.

Documentation

Comprehensive documentation for VAM consists of an administration and user's guide that provides installation and configuration information, along with product release notes that contain late-breaking product information. Documentation is available in HTML and PDF formats on the Process Software Web site, www.process.com.

You can find Frequently Asked Questions (FAQs) on the Tech Support web page on the Process Software web site.

Ordering Information

VAM is downloaded from Process Software. Contact sales@process.com or request a free evaluation on the Process Software web site at www.process.com.

Hardware and Software Requirements

VAM requires at least one network controller supported by MultiNet, TCPware or TCP/IP Services.

VAM supports the following operating system versions:

- OpenVMS Alpha 8.2 and higher
- OpenVMS Integrity 8.2 and higher

VAM supports the following TCP/IP stacks and versions:

- MultiNet V5.4 and later
- TCPware V5.9 and later
- TCP/IP Services v5.5 or later

© Process Software Corporation and/or its affiliates. All rights reserved.

About Process Software

Process Software is a premier supplier of infrastructure software solutions to mission critical environments. We deliver customer-centric and innovative IP-based technologies to our customers worldwide, and provide them with superior customer support and service.

Process Software
959 Concord Street
Framingham, Massachusetts 01701-4682

Telephone:
U.S./Canada 1- (800) 722-7770
International 1- (508) 879-6994

FAX: 1- (508) 879-0042

Web: http://www.process.com

E-mail: info@process.com

The information contained in this document is subject to change without notice. Process Software assumes no responsibility for any errors that may appear in this document.

© Process Software, All rights reserved

The Process Software name and logo are trademarks, and TCPware, MultiNet, PMDF, and PreciseMail Anti-Spam are registered trademarks of Process Software. All other company names and product names are trademarks or registered trademarks of their respective holders.