Layer7 Privileged Access Manager v3.3 Release Announcement

May 20th, 2019

To: Layer7 Privileged Access Manager (PAM) Customers
From: The Layer7 Privileged Access Manager Product Team
Subject: Announcing the Release of Layer7 Privileged Access Manager v3.3

On behalf of CA Technologies, we appreciate your business and the opportunity to provide you with high-quality, innovative software and services. As part of our ongoing commitment to customer success, we regularly release updated versions of our products. Today, we are pleased to announce the release of Layer7 Privileged Access Manager (Layer7 PAM) v3.3. This release includes significant new capabilities designed to extend support for hybrid enterprise protection and enhance security and integration.

New features for Layer7 PAM 3.3 include:

- **New Clustering Replication Architecture**

Layer7 PAM now has a new replication architecture designed to minimize downtime. The new clustering architecture provides you with:

- Reduced downtime for maintenance: Adding and removing sites and members without stopping the cluster
- Extended self-healing of out-of-sync cluster members
- Reduced vulnerability to "split-brain" scenarios
- Added Secondary Site leaders to distribute replication among each site, reducing WAN traffic
- Ability to purge logs of all members in a site from any site member

- **Custom Connector Framework**

Layer7 PAM provides out-of-the-box application types and target connectors, which might not be sufficient for your remote systems and applications. For remote targets that are not available out-of-the-box, you can build custom target connectors using the Custom Connector Framework.

- **Cryptographic Algorithms for SSH Communication**

This release supports the latest recommended strong cryptography algorithms for secure SSH communications. These algorithms are included with the following Layer7 Privileged Access Manager components, which use SSH:

- SSH access method
- Cisco target connector for credential management
- UNIX target connector for credential management

- **PIV/CAC Custom Field Mapping for Active Directory**

You can now map specific fields from PIV/CAC smart cards to fields in Active Directory for authentication. You can configure the smart card Subject Name and Subject Alt Name fields to various supported AD attributes on the new Custom Field Mapping tab.

- **Azure Active Directory Support**

Use the Azure Active Directory (AD) connector to update the passwords of Azure AD accounts.

- **Exclusive Checkout for Auto-Connect**

Exclusive Checkout on Auto Connect allows users to check out the account exclusively. The account is checked out when the user opens a connection to the target account. This account is only checked in when all the open connections to the account are closed by the user.

- **Enhanced Security for the LDAP Browser**

Security for the LDAP Browser is improved. The LDAP Browser now supports the following features:

- Communication using cipher suites that support Perfect Forward Secrecy
- Enforcement of FIPS mode
- Support for disallowing TLS 1.0/1.1 connections

- **Enable Multiple Accounts for a Transparent Login Connection**

Within a policy, you can associate multiple Target Accounts for use as Transparent Login Credentials (TLC) for a Transparent Login enabled RDP Application Service (TL Service). Previously, only a single account could be associated as a TLC for each TL Service in a policy. Now, TLC for a policy containing a TL Service is decoupled from the TL Service Windows. This was not supported previously, as only one TLC tied to a specific device could be used.

- **Retrospective Approval for Password View Requests**

Configure password view policies with the new *retrospective approval* option to allow immediate "break glass" access to account credentials. When such credentials are viewed, a notification is sent to administrators with an approver role for after-the-fact approval.

- **Compressed Database Backups**

Database backups are now performed in one step. Instead of copying the file and then compressing it, the file is compressed as it is copied. This method requires less disk space.

- **Support for Azure U.S. Government Cloud Type**

This release supports The Azure US Government Cloud type which provides access to Azure.gov features from on-premise PAM instances.

- **New SCIM API Integration**

SCIM (System for Cross-domain Identity Management) is an application-level REST protocol for managing user identity data between domains. The Layer7 PAM REST API now includes a SCIM section.

- **Expiration Time for Access to Remote Debugging Services**

For enhanced security, you can set an expiration date for access to Remote Debugging Services.

- **Updated Layer7 PAM Client for MacOS**

The updated Layer7 PAM Client for the macOS is easier to install and use. The updated Mac client is a native Mac app that now supports High Sierra and Mojave. The new client has privilege separation, and you no longer have to download the Layer7 PAM Assistant to install it.

- **New Layer7 PAM Agent for Windows 10 Desktops**

The Layer7 PAM Agent is a lightweight Windows alternative to the Layer7 PAM Client. The PAM Agent:

- Does not use Java applets
- Enables end users to use the Windows applications that they already have
- Tunnels through LAYER7 Privileged Access Manager to devices, allowing auto-login and session recording
- Does not require the configuration of loopback addresses
- Does not contain a browser, so it does not support Layer7 Privileged Access Manager administration
- Has a much smaller installer, storage footprint, and memory requirement
- Uses Services instead of Access Methods

- **New SNMP Traps**

Two new SNMP traps provide information about disk space usage and database usage. A timer task in Java runs every hour and generates the following alerts:

- gkTotalDiskUsageStatus - Total Disk Used. Example: Total Disk Used: 41% (4.01GB of 9.64GB)
- gkTotalDBDiskUsageStatus - Total DB Disk Used. Example: Total DB Disk Used: 17383424

CA plans to support the Layer7 Privileged Access Manager v3.3 release, including all subsequent service packs, until **May 20th, 2021.** Please consider this letter your written notification of End of Service of the Layer7 Privileged Access Manager v3.3 release, effective **May 20th, 2021**.

NOTE: Please refer to the upgrade prerequisites when planning your upgrade. The link to the online documentation is located here:

https://docops.ca.com/ca-privileged-access-manager/3-3/EN/upgrading/upgrade-to-release-3-3/upgrade-prerequisites-for-3-3

We encourage you to visit the Layer7 PAM product information page on the CA Support Online website at https://support.ca.com/ for more information. If you have any questions or require assistance contact CA Customer Care online at http://www.ca.com/us/customer-care.aspx where you can submit an online request using the Customer Care web form: https://support.ca.com/irj/portal/anonymous/customercare. You can also call CA Customer Care at +1-800-225-5224 in North America or see http://www.ca.com/phone for the local number in your country.

To learn about the new features offered in Layer7 PAM 3.3, refer to the product documentation at docops.ca.com. To connect, learn and share with other customers, join and participate in our Layer7 Privileged Access Manager CA Community at https://communities.ca.com/. To review CA Support lifecycle policies, please review the CA Support Policy and Terms located at: https://support.ca.com/.

Thank you again for your business.