DATA SHEET

CA Privileged Access Manager for VMware NSX

At a Glance

Quickly deployable and delivering fast time-to-protection, CA Privileged Access Manager enhances security, facilitates compliance and minimizes costs. Tightly integrated with native NSX security facilities, CA Privileged Access Manager for VMware NSX delivers critical privileged access management, designed to prevent breaches by limiting privileged user activities, dynamically controlling access to resources—including the sensitive NSX Manager, proactively enforcing security policies and automatically modifying them as circumstances change, protecting sensitive administrative credentials and monitoring and recording privileged user activity across all IT infrastructure.

Key Benefits/Results

- Control privileged access across all resources.
- Deploy solution quickly.
- Automatically discover and protect virtual assets.
- Dynamically modify access controls in response to security posture changes.
- Protect VMware NSX manager and controllers.
- Manage privileged account credentials and single sign-on.
- Monitor, react and record activities.

Key Features

- Automatic discovery of VMware NSX resources.
- Protection of VMware NSX Manager and Controllers, and all other IT resources
- Dynamically linked security groups
- Service Composer Integration
- Distributed Firewall Access Restrictor
- NSX REST API Proxy
- Unified cross-platform privileged user credentials protection
- Monitoring, audit trail, session recording and reporting
- Security and privacy regulatory support
- Full attribution of actions to individuals and separation of duties
- Multifactor authentication, single sign-on, and federation support
- Interoperability with active directory, LDAP, Radius, TACACS+ and other identity stores

Business Challenges

Many data breaches happen because of compromises in privileged user accounts. Standards and regulation bodies, as well as auditors, have recognized the risks associated with privileged users and have introduced regulatory changes and audit standards to mitigate these risks. Yet risks are spreading like wildfire in growing dynamic and distributed virtualized and cloud environments common in enterprise IT today. Uncontrolled access to NSX resources provides privileged users with the ability to delete or modify network resources en masse and make sweeping configuration and operational changes to the environment. One improperly authorized privileged account can cause widespread and irreparable damage to an organization's infrastructure, intellectual property and brand equity, leading to sudden drops in market value and broad organizational disruption.

Solution Overview

CA Privileged Access Manager is a simple-to-deploy, automated, proven solution for privileged access management in physical, virtual and cloud environments. Available as an Open Virtualization Format (OVF) virtual appliance and fully integrated with VMware management environment, CA Privileged Access Manager for VMware NSX enhances NSX native security by controlling privileged access and limiting sensitive administrative activities in VMware NSX Manager and the NSX REST API by monitoring and recording privileged user activity, proactively enforcing separation of duties, providing full password and credential management and enabling a single point of privileged identity management for all of VMware and other IT resources. CA Privileged Access Manager is designed to protect the physical data center assets, virtual infrastructure, private cloud, public cloud and hybrid environments with one scalable, agentless solution, providing centralized access across tools and resources.

Critical Differentiators

CA Privileged Access Manager for VMware NSX enhances VMware NSX's native security capabilities and adds fine-grained access control.

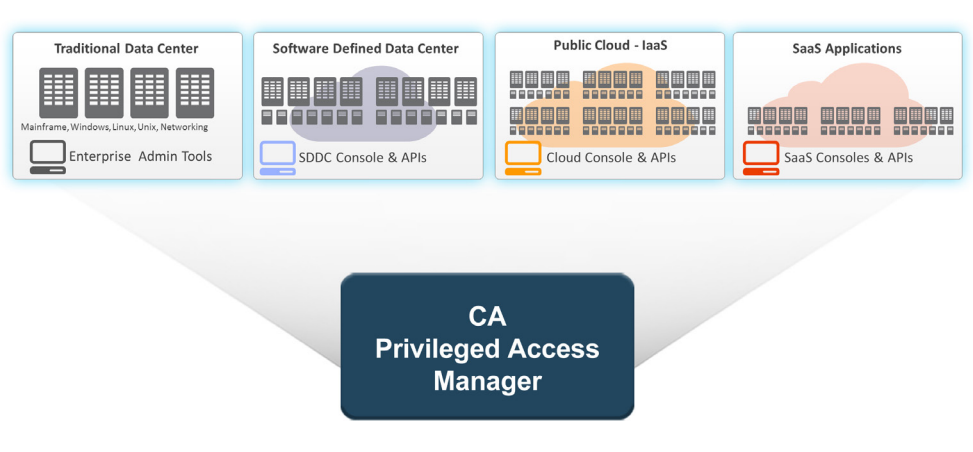
Automatically discover and protect ESX/ESXi hosts and guest systems. Automatically establish and enforce policies across dynamic virtual resources by adding policy protections and access permissions in real-time, as virtual instances are created.

Automatically define highly restrictive, micro-segmented, secure network access to NSX-based resources. Using synchronized security settings deep inside NSX Security Groups, automatically provide short-term administrative access to select systems—or deny access and terminate sessions in response to security incidents.

Monitor, react and record everything, including NSX REST APIs interactions. Deliver full audit and response logs of all user events, including interactions with the powerful NSX Manager APIs. Capture continuous, tamper-evident logging and recording of administrative sessions. Generate alerts, warnings or even terminate sessions. Analyze logs using VMware vRealize Log Insight or other log managers.

Manage privileged user credentials and simplify with single sign-on. Vault credentials in an encrypted credential safe. Gain faster access and productivity improvements with single sign-on.

CA Privileged Access Manager



Supported Environments

- **CA Privileged Access Manager delivers** privileged access capabilities across a range of IT infrastructure, including Linux®, Microsoft Windows®, UNIX®, networking devices, multiple databases and business applications, and more. Optional extensions provide enhanced integration with VMware vSphere vCenter Server and guest systems, NSX software-defined networks, IBM® mainframes, Microsoft Office® 365 Admin Center and Amazon Web Services (AWS), including the AWS Management Console and APIs.

Related Products/Solutions

- **CA Privileged Access Manager server control** provides a comprehensive solution for protecting extremely critical business assets with fine-grained protections over operating system-level access and application-level access.

For more information, please visit **ca.com/security**

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

CS200_163434_1115