WHITE PAPER: PRIVATE MANAGED CAS STREAMLINE INTERNAL SERVER CERTIFICATE MANAGEMENT

White Paper

Private Managed CAs Streamline Internal Server Certificate Management

Symantec

Norton SECURED powered by Symantec

Private Managed CAs Streamline Internal Server Certificate Management

CONTENTS

Private Managed CAs Streamline Internal Server Certificate Management

Digital certificates are fundamental components of IT information systems. They are widely used for both authentication and encryption. Due to changes in rules governing the use and issuance of Secure Sockets Layer (SSL) certificates, many companies and organizations will have to change how they use internal certificates.

Certificates With Internal Names and Changing Rules

An SSL certificate with an internal name is one that is used on a private domain, that is, one ending in a non-standard suffix, such as *db-server1.mycompany.local*, or a reserved IP address. Private networks in IPv4 are in the ranges of 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. The IPv6 address block of fc00::/7 has been reserved for similar purposes.

According to the Certification Authority/Browser Forum (CA/BF) baseline requirements (9.2.1), beginning in November 2015, CAs will no longer issue SSL certificates with internal names such as *db-server1.mycompany.local.* As of October 2016, all such certificates that are unexpired will be revoked.

These rule changes do not mean that internal certificates are no longer available for use, only that public CAs cannot issue certificates with internal names that are not authenticated. Companies and other organizations that want to use internal-named certificates are welcome to do so–as long as they have their own CA. There are two options for having you own CA: implement an in-house self-signed CA or use a third-party CA service.

Although running your own CA might sound appealing, to those inclined to the do-it-yourself (DIY) approach to IT operations, there are a number of factors to consider.

Challenges to Maintaining a Self-Signed CA

A self-signed CA is part of a private key infrastructure (PKI), a complex set of technologies that pose several challenges:

- Need for technical knowledge
- Ability to secure CA infrastructure
- Management overhead
- Unanticipated costs
- Increased Risks

Each of these challenges can undermine a company's ability to deliver secure certificate services or could drive up the cost of implementing an in-house solution for internal server certificates.

Technical Knowledge
Managing a CA requires knowledge to install certificate management applications or develop your own home-brewed applications. These include applications to generate a root certificate as well as generate and distribute certificates for individuals and servers. Additionally, there is an increase in risk with unexpected SSL certificate expirations and key compromise.

Ability to Secure CA Infrastructure
Perhaps one of the most challenging aspects of managing your own CA is securing the CA infrastructure. Doing so begins with hardening the operating system (OS) of the server running your CA application. The server should have only the applications and daemons needed to support its function. Unneeded ports should be closed. Vulnerability scans should be run regularly, and software patched as needed.

In addition, controls need to be in place to prevent a breach from an insider. Administrators and others with access to the CA servers should have the least privileges required to do their job. This setup often means root or administrator privileges, so it is important to follow other security best practices, such as the rotation of duties and continuous monitoring of significant events on the server. Regular audits should be performed as well.

Administrators will need to control access to passwords used to secure the server and to create certificates. Although access to such passwords should be minimized, it is also important that multiple individuals have access so that someone is always likely to be available with that knowledge when needed.

Management Overhead
Much of the management overhead in maintaining a CA is dedicated to securing the server and the information on it. Other overhead includes the processes and procedures that need to be designed and implemented to verify requests for certificates, certificate database management, and other systems administration tasks, such as performing backups and planning for disaster recovery.

Unanticipated Costs
Unanticipated costs can occur when certificates expire prior to being replaced. This expiration can disrupt operations and lead to internal downtime.

Other costs, such as maintaining a failover server in a disaster recovery site and the cost of maintaining replication procedures so that the failover server is in synch with the production server, can drive up the cost of maintaining your own CA.

Although organizations can choose to run their own PKI, it might be more cost effective to use an internal certificate service.

Private CA Service

A CA service is a type of software as a service (SaaS) that alleviates many of the management and security concerns of running a private, internal CA in-house. A CA as a service combines the best features of a CA with the benefits of expert CA providers.

The advantages include:

- Minimal technical knowledge of CA and PKI is required to start
- CA service providers create and manage CAs for your business; CAs are not shared among customers
- CA is run by experts who understand both security and infrastructure
- The CA service provider is responsible for securing CA servers and the network as well as implementing appropriate access controls
- A CA service eliminates the need for additional hardware, reducing the capital expenditures needed to support internal certificates
- CA service providers can offer tools, such as consolidated management of certificates
- This approach delivers rapid time to deployment because all the hardware, software, and network services are already in place

CA management is emerging as another IT function that is available as a service. The economics of leveraging consolidated service operations is driving many companies to adopt SaaS products. This new way of delivering IT services is helping reduce capital costs, improve the quality of service, and reduce unnecessary management overhead in the data center.

Conclusions

The CA/BF, the governing body that manages the use of SSL certificates, has determined that public CAs will no longer issue certificates with internal names after November 2015. The logic for using SSL certificates has not changed, but organizations will have to adopt new ways of issuing them. Users of non-compliant certificates have two choices: they can implement their own internal CA or they can turn to experts who can run a private CA for them. The former option requires technical knowledge, the ability to secure and manage infrastructure, and could incur upfront costs as well as ongoing management and administration costs. Alternatively, providers that offer a private CA can leverage the economic and technical advantages without the need for onsite expertise, hardware, or software.

More Information

Visit our website

https://www.symantec.com/private-ssl

To speak with a Product Specialist

North America:	+1(866) 893-6565 or	
	+1(520) 477-3135	SSL_EnterpriseSales_NA@symantec.com
U.K. and Ireland:	+0800 032 2101	sslsales-uk@symantec.com
Rest of EMEA:	+353 1 793 9053 or	
	+41 (0) 26 429 7929	sslsales-ch@symantec.com
Asia Pacific:	+61 3 9674 5500	ssl_sales_APAC@symantec.com

To speak with a Product Specialist outside the U.S.

To speak with additional product specialists around the world, visit our website for specific offices and contact numbers.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

UID: 228/08/14