

CLAIMS

What is claimed is:

1. An application centric centralized certificate management system for managing a plurality of certificates on granular object level in a plurality of datacenters, said application centric centralized certificate management system comprising:

a memory unit that stores a database and a set of modules; and

a hardware processor that executes said set of modules, wherein said set of modules comprise:

a discover module, executed by said hardware processor, configured to discover said plurality of certificates;

an inventory module, executed by said hardware processor, configured to provide details of said discovered plurality of certificates;

a work order module, executed by said hardware processor, configured to store details of (i) a work order id of said plurality of certificates, (ii) device information of said plurality of certificates, (iii) a time stamp of implementation of said plurality of certificates, and (iv) a status of said plurality of certificates;

a policy module, executed by said hardware processor, configured to create a policy that specifies (i) an usage of said plurality of certificates, and (ii) practices that a certificate authority (CA) employs to manage said plurality of certificates, wherein said policy module is configured to perform a compliance check against said plurality of certificates based on said policy to generate compliance reports for plurality of certificates;

a new certificate module, executed by said hardware processor, configured to create a new certificate; and

a validation module, executed by said hardware processor, configured to validate (a) said new certificate when said new certificate is added to said application centric centralized certificate management system, and (b) said plurality of certificates; and

a display unit that displays a holistic view of said plurality of certificates to perform one or more actions on granular object level.

2. The application centric centralized certificate management system of claim 1, wherein said set of modules comprises;

a certificate group module, executed by said hardware processor, configured to create a certificate group for said plurality of certificates; and

a settings module, executed by said hardware processor, configured to manage authentication details to initiate a secured connection with a certificate authority to perform one or more actions on said plurality of certificates.

3. The application centric centralized certificate management system of claim 1, wherein said inventory module is configured to provide an option to associate said plurality of certificates to said certificate group.

4. The application centric centralized certificate management system of claim 1, wherein said policy is applied to said plurality of certificates on granular object level by associating said policy to said certificate group.

5. The application centric centralized certificate management system of claim 1, wherein said discover module is configured to discover said plurality of certificates based on at least one of (i) an IP range, (ii) a subnet, (iii) an URL, (iv) by uploading a certificate, and (v) managed devices.

6. The application centric centralized certificate management system of claim 1, wherein said policy module is configured to perform at least one action on granular object level, wherein said at least one action is selected from a group comprising:

- (a) providing access control to said plurality of certificates; and
- (b) a policy enforcement on said plurality of certificates.

7. The application centric centralized certificate management system of claim 2, wherein said new certificate module is configured to provide an option to select a connector type for creating said new certificate.

8. A non-transitory program storage device readable by computer, and comprising a program of instructions executable by said computer to perform a method for managing a plurality of certificates on granular object level in a plurality of application specific networking components across a plurality of data centers, said method comprising:

discovering a plurality of certificates in said application centric centralized certificate management system;

providing details of said plurality of certificates;

storing details of (i) a work order id, (ii) a device information, (iii) a time stamp of implementation, and (iv) a status associated with said plurality of certificates;

creating a policy for said plurality of certificates;

performing compliance check against said plurality of certificates based on said policy to generate compliance reports for said plurality of certificates;

creating a group to categorize said plurality of certificates;

managing authentication details to initiate a secured connection with a certificate authority to perform one or more actions on said plurality of certificates;

creating a new certificate; and

validating (a) said new certificate when said new certificate is added to said application centric centralized certificate management system, (b) said plurality of certificates.

9. The non-transitory machine-readable medium of claim 8, wherein said method further comprises displaying a holistic view of said plurality of certificates to perform one or more actions on granular object level, wherein said one or more actions comprises (i) performing validation check on said plurality of certificates, (ii) renewing said plurality of certificates, (iii) revoking said plurality of certificates, or (iv) pushing said plurality of certificates.

10. The non-transitory machine-readable medium of claim 8, wherein said policy is applied to said plurality of certificates on granular object level by associating said policy to said certificate group.

11. A computer implemented method for managing a plurality of certificates on granular object level in a plurality of application specific networking components across a plurality of data centers using an application centric centralized certificate management system, said method comprising:

- discovering a plurality of certificates in said application centric centralized certificate management system;

- providing details of said plurality of certificates;

- storing details of (i) a work order id, (ii) a device information, (iii) a time stamp of implementation, and (iv) a status of said plurality of certificates;

- creating a policy for said plurality of certificates;

- performing compliance check against said plurality of certificates based on said policy to generate a compliance reports for said plurality of certificates;

- creating a group to categorize said plurality of certificates;

- managing authentication details to initiate a secured connection with a certificate authority to perform one or more actions on said plurality of certificates;

- creating a new certificate; and

- validating (a) said new certificate when said new certificate is added to said application centric centralized certificate management system, and (b) said plurality of certificates.

12. The computer implemented method of claim 11, further comprising displaying a holistic view of said plurality of certificates to perform one or more actions on granular object level, wherein said one or more actions comprises (i) performing validation check on said plurality of certificates, (ii) renewing said plurality of certificates, (iii) revoking said plurality of certificates, or (iv) pushing said plurality of certificates.