SECURING A CLUSTER

Fast Lane

Understanding Nutanix's Approach to Security

In deze module maakt u kennis met verschillende beheertaken die u op VM's kunt uitvoeren, variërend van het uitvoeren van eenvoudige configuratie-updates en het bijwerken van VM-plaatsingsregels tot het automatiseren van basisbeheertaken.

SECURITY FEATURES

Fast Lane

- How security is built into the Nutanix platform from the ground up.
- How STIGs and SCMA are used and automated to self-heal a cluster using security baselines.
- How to configure authentication in Prism Central via a directory service or a SAML-based identity provider.
- How to enable and configure client (that is, two-way) authentication.
- How to create and manage local user accounts in Prism Central.
- What role-based access control is.
- What cluster lockdown is.
- What Flow Network Security is, how security polices work, and what types of security policies are available.
- How Nutanix implements both hardware and software-based data-at-rest encryption.

In deze module maakt u kennis met verschillende beveiligingsfuncties die Nutanix biedt, waaronder authenticatie, het maken van gebruikersaccounts, op rollen gebaseerde toegangscontrole, clustervergrendeling en versleuteling van gegevens in rust.
Hoe beveiliging vanaf het begin is ingebouwd in het Nutanix-platform.

Hoe STIG's en SCMA worden gebruikt en geautomatiseerd om een cluster zelf te herstellen met behulp van beveiligingsbasislijnen.

Verificatie configureren in Prism Central via een directoryservice of een op SAML gebaseerde identiteitsprovider.

Clientverificatie (dat wil zeggen tweerichtingsverificatie) inschakelen en configureren.

Lokale gebruikersaccounts maken en beheren in Prism Central.

Wat op rollen gebaseerde toegangscontrole is.

Wat clusterlockdown is.

Wat Flow Network Security is, hoe beveiligingsbeleid werkt en welke soorten beveiligingsbeleid beschikbaar zijn.

Hoe Nutanix zowel hardware- als softwaregebaseerde data-at-rest encryptie implementeert.

HOW DOES NUTANIX APPROACH SECURITY

Fast Lane

Protection strategies

- Per VM Backup
- Selective, Bi-directional ReplicationAt the file level
- Synchronous Datastore Replication: Datastores can be spanned across two sites to provide seamless protection in the event of a site disaster.

Nutanix integreert beveiliging in elke stap van productontwikkeling, via een aanpak die de security development lifecycle (SecDL) wordt genoemd. In plaats van beveiliging toe te passen als een bijzaak, is de SecDL een fundamenteel onderdeel van het productontwerp.

De sterk doordringende cultuur en processen die rond beveiliging zijn gebouwd, versterken de Nutanix Enterprise Cloud en elimineren zero-day kwetsbaarheden. Efficiënte bewerkingen met één klik en zelfherstellende beveiligingsmodellen maken eenvoudig automatisering mogelijk om de beveiliging te handhaven in een hypergeconvergeerde oplossing die altijd actief is.

Nutanix voldoet aan RHEL 7 Security Technical Implementation Guides (STIG's) die machineleesbare code gebruiken om naleving van strenge gemeenschappelijke normen te automatiseren. Met Nutanix Security Configuration Management Automation (SCMA) kunt u uw platform snel en continu beoordelen en herstellen om ervoor te zorgen dat het aan alle wettelijke vereisten voldoet of deze overtreft.

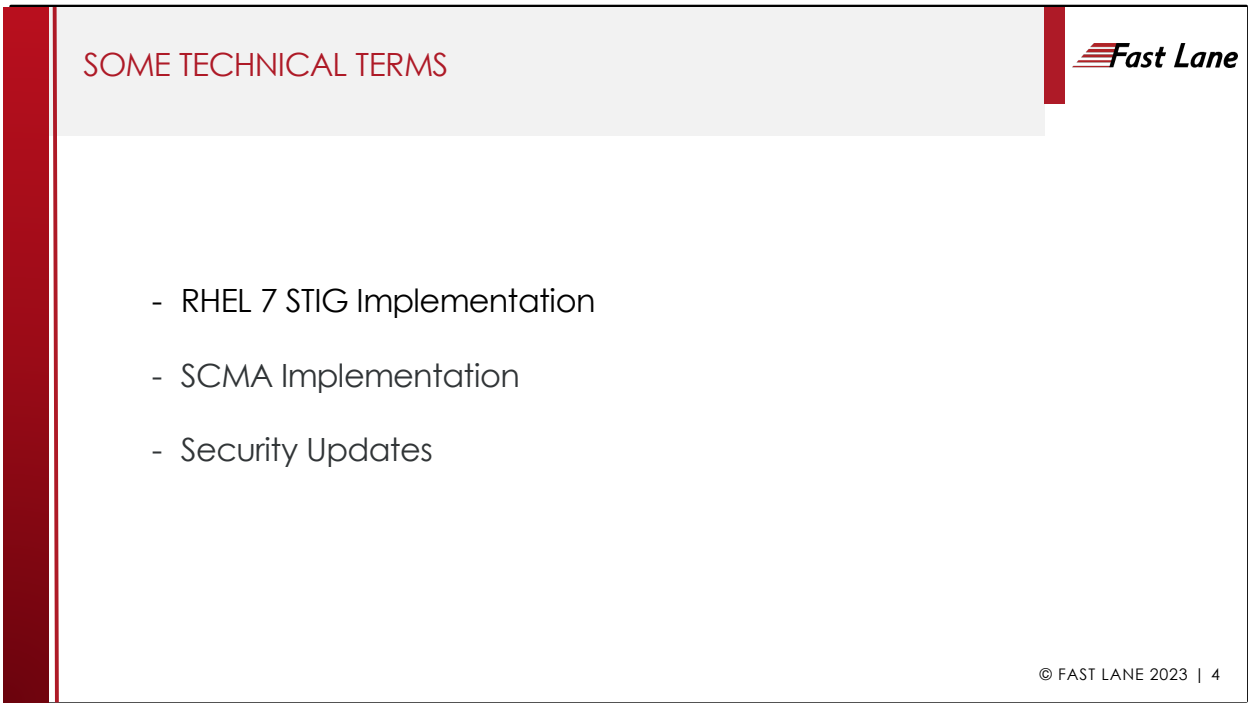
Nutanix heeft het beveiligingsprofiel van de Controller VM gestandaardiseerd tot een basislijn voor beveiligingsnaleving die voldoet aan of beter is dan de standaard

vereisten voor hoog bestuur. De meest gebruikte referenties in de Verenigde Staten voor beveiligingsgerelateerde technische vereisten zijn:

Het National Institute of Standards and Technology Special Publications Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800.53)

Het Amerikaanse Department of Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)

Evenzo is in Europa/EMEA een veelgebruikte norm waaraan Nutanix voldoet, het ISO 270001-raamwerk.



RHEL 7 STIG-implementatie

–

De Nutanix Controller VM ondersteunt STIG-compliance met de RHEL 7 STIG zoals gepubliceerd door DISA. STIG-regels zijn in staat om de bootloader, pakketten, het bestandssysteem, opstarten en servicebeheer, bestandseigendom, authenticatie, kernel en logboekregistratie te beveiligen.

SaltStack en SCMA worden gebruikt om elke afwijking van de beveiligingsbasislijnconfiguratie van het besturingssysteem en de hypervisor zelf te herstellen om in overeenstemming te blijven. Als een onderdeel niet-compatibel is, wordt het onderdeel teruggezet naar de ondersteunde beveiligingsinstellingen zonder handmatige, administratieve tussenkomst.

SCMA-implementatie

–

Het Nutanix-platform en alle producten maken gebruik van het Security Configuration Management Automation (SCMA)-framework om ervoor te zorgen dat services voortdurend worden geïnspecteerd op afwijkingen van het beveiligingsbeleid. SCMA controleert meerdere beveiligingsentiteiten voor zowel Nutanix-opslag als AHV,

rapporteert en registreert automatisch inconsistenties en zet entiteiten vervolgens terug naar de basislijn indien nodig.

Met SCMA kunt u de STIG zo plannen dat deze elk uur, dagelijks, wekelijks of maandelijks wordt uitgevoerd. Het uitvoeren van de STIG heeft geen invloed op de systeemprestaties, aangezien het de laagste systeemprioriteit heeft binnen de virtuele opslagcontroller, waardoor u zo vaak controles kunt uitvoeren als uw bedrijfsbeleid vereist.

Beveiligingsupdates
–
Nutanix biedt continue fixes en updates om bedreigingen en kwetsbaarheden aan te pakken. Nutanix-beveiligingsadviezen bieden gedetailleerde informatie over de beschikbare beveiligingsfixes en -updates, inclusief de kwetsbaarheidsbeschrijving en de getroffen product/versie.

Als u de lijst met beveiligingsadviezen wilt bekijken of naar een specifiek advies wilt zoeken, meldt u zich aan bij de SupportPortal en selecteert u Documentatie en vervolgens Beveiligingsadviezen.

SECURING WITH PRISM CENTRAL

Fast Lane

- Active Directory or OpenLDAP
- SAML
- Local user authentication

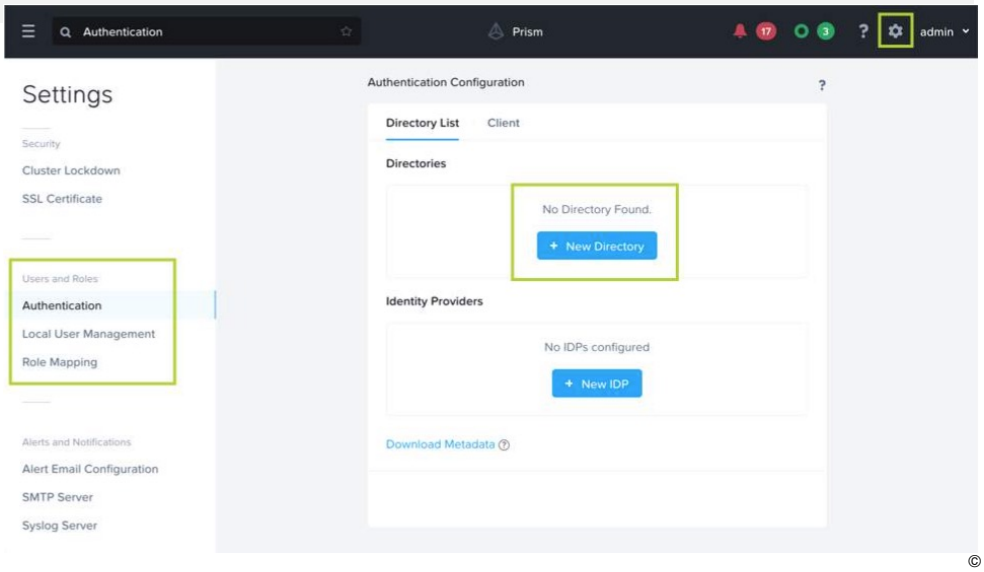
Prism Central ondersteunt deze opties voor gebruikersauthenticatie (elk van deze drie opties wordt in deze sectie besproken):

Active Directory of OpenLDAP: Gebruikers kunnen authenticeren met hun Active Directory- of OpenLDAP-referenties als ondersteuning is ingeschakeld voor Prism Central.

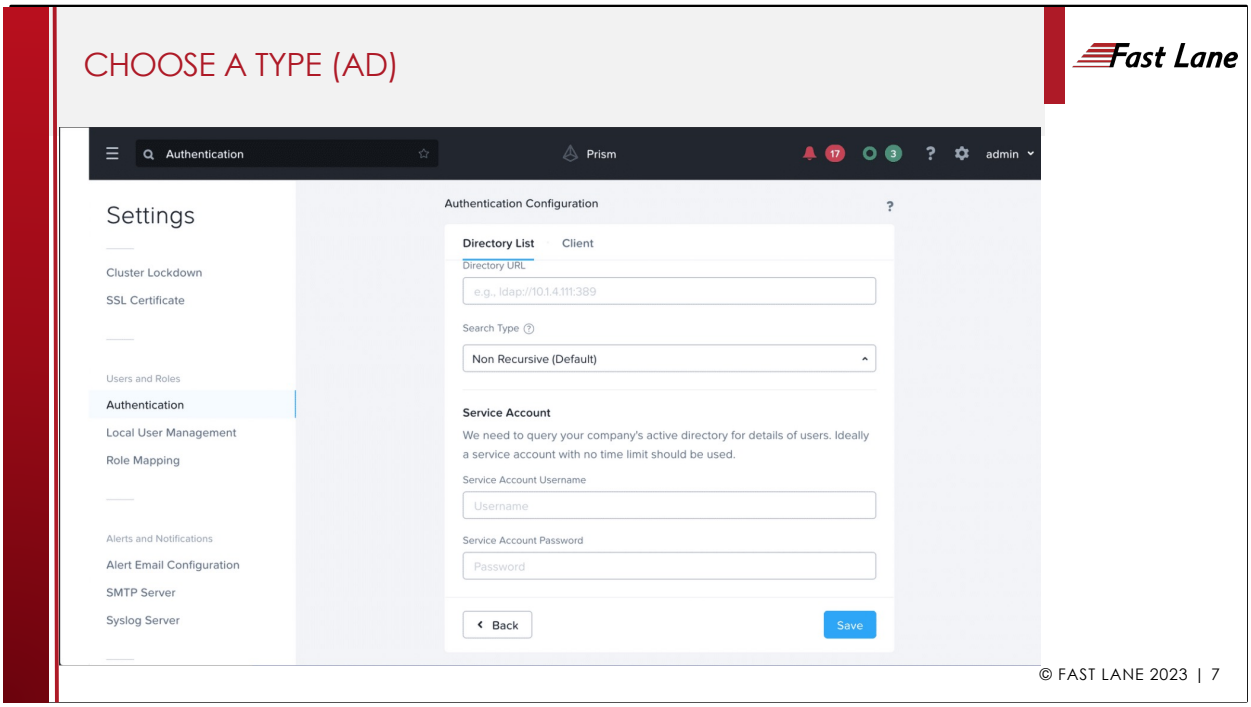
SAML: Gebruikers kunnen authenticeren via een ondersteunde identiteitsprovider als SAML-ondersteuning is ingeschakeld voor Prism Central.

Lokale gebruikersauthenticatie: Gebruikers kunnen authenticeren als ze een lokaal Prism Central-account hebben.

ADDING AN AUTHENTICATION DIRECTORY

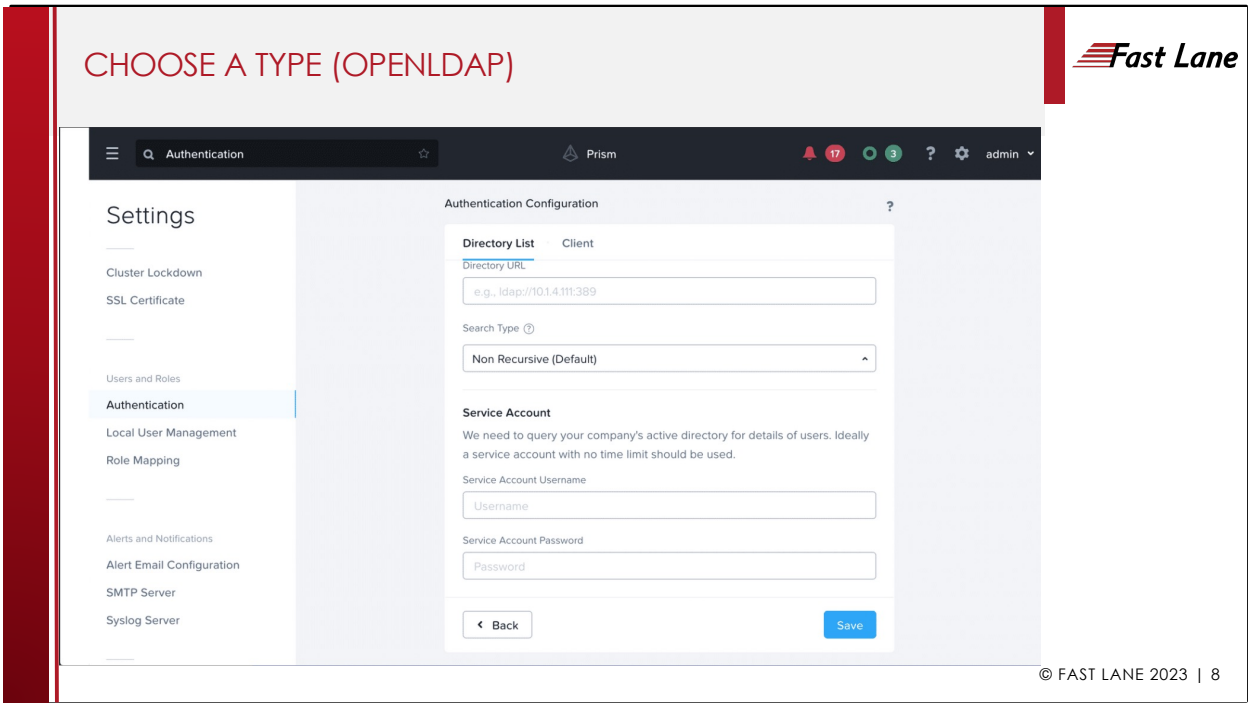


Om een nieuwe adreslijstservice toe te voegen, klikt u in de categorie Gebruikers en rollen op Verificatie.
Wanneer het dialoogvenster Authenticatieconfiguratie wordt weergegeven, klikt u in het gedeelte Directory's op + Nieuwe directory.



Choosing a Directory Type (Active Directory)

Eerst wordt u gevraagd een directorytype te kiezen. De opties in de rest van het dialoogvenster veranderen op basis van uw selectie. Als u bijvoorbeeld Active Directory selecteert, moet u een naam, domein, directory-URL, zoektype en serviceaccount opgeven, zoals weergegeven in de volgende afbeelding.



Choosing a Directory Type (OpenLDAP)

Aan de andere kant, als u OpenLDAP selecteert, wordt u naast de hierboven vermelde informatie ook gevraagdom de gebruikersobjectklasse, gebruikerszoekbasis, gebruikersnaamattribuut, groepsobjectklasse, groepszoekbasis, groepslidkenmerk en attribuutwaarde van groepslid.

CONFIGURING AN IDP

Fast Lane

Key features of IAM are:

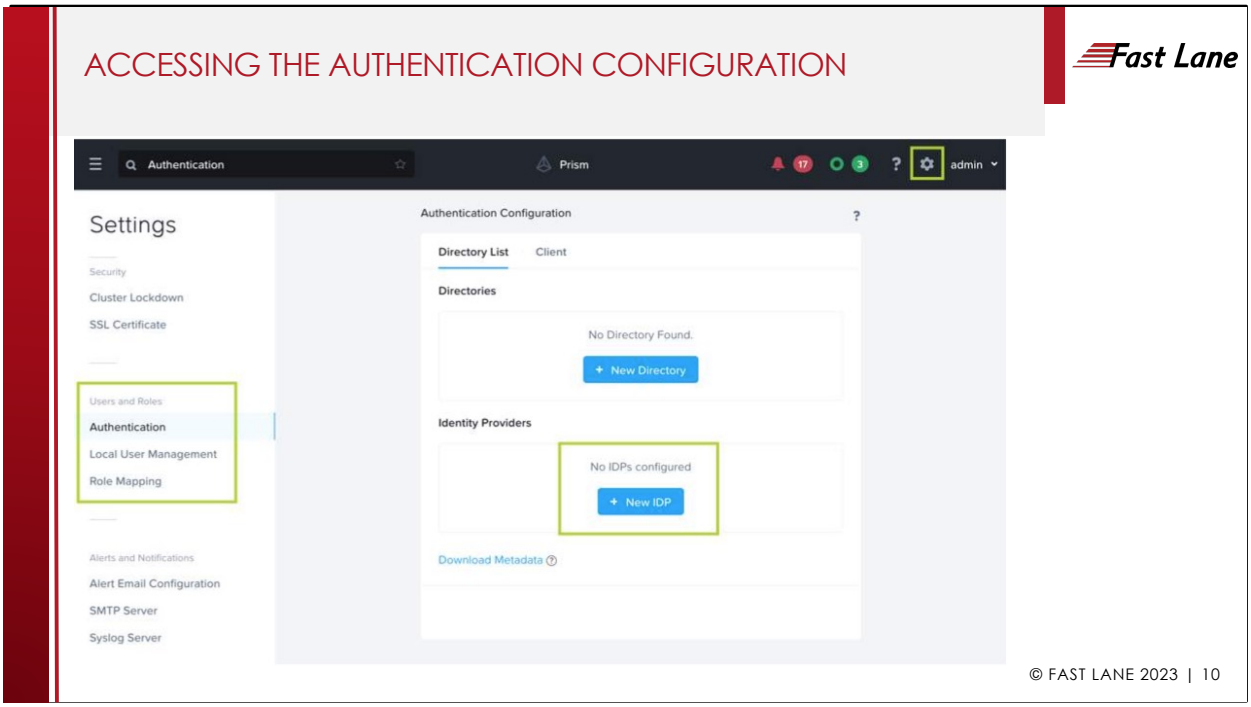
•Highly Scalable Architecture. IAM is based on Kubernetes, and uses independent pods for authentication, authorization, and IAM data storage and replication.

•Secure by Design. Mutual TLS authentication (mTLS) secures IAM component communication. The Micro Services infrastructure on Prism Central provisions certificates for mTLS.

•More SAML identity providers. As described earlier, enabling IAM allows you to use IDPs beyond just ADFS.

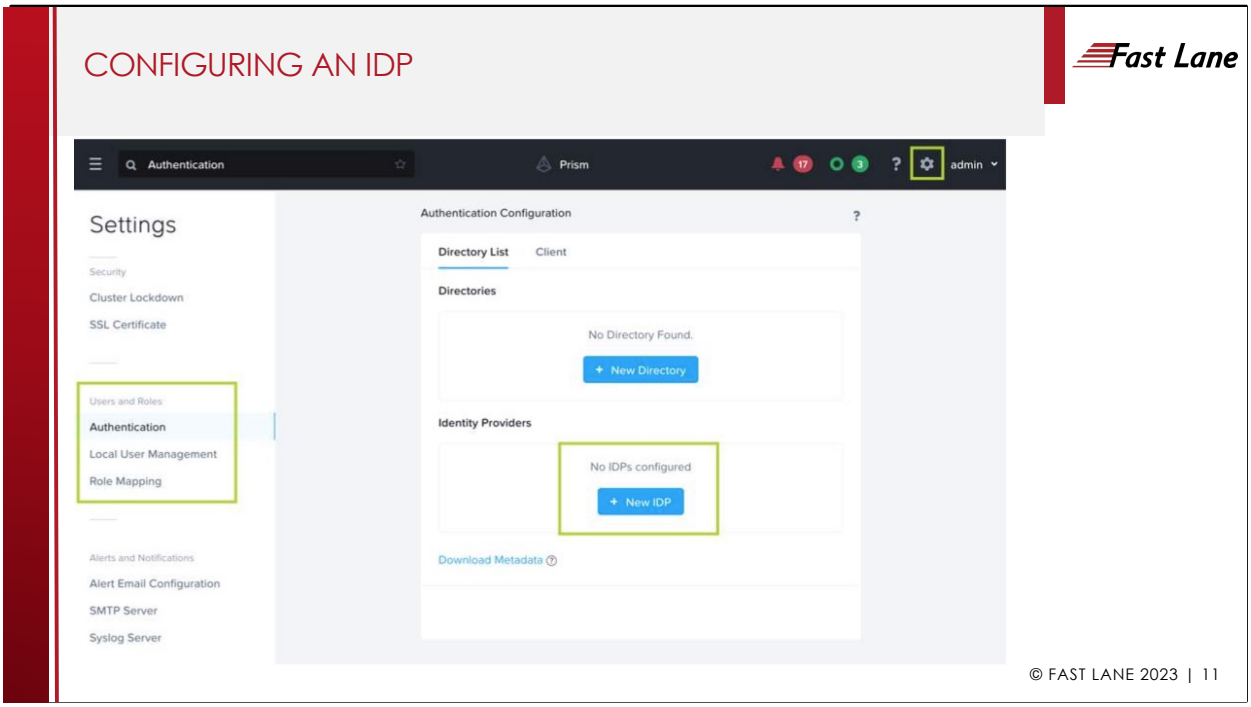
Identity and Access Management (IAM) is een authenticatie- en autorisatiefunctie die kan worden ingeschakeld en beheerd in Prism Central.
Het maakt gebruik van op attributen gebaseerde toegangscontrole (ABAC) en is standaard uitgeschakeld.

Als IAM niet is ingeschakeld, is Active Directory Federations Services (ADFS) de enige ondersteunde IDP voor eenmalige aanmelding.
Als IAM is ingeschakeld, zijn er meer opties beschikbaar, waaronder Azure ADFS, Okta, PingOne, Shibboleth en Keycloak.



Accessing the Authentication Configuration

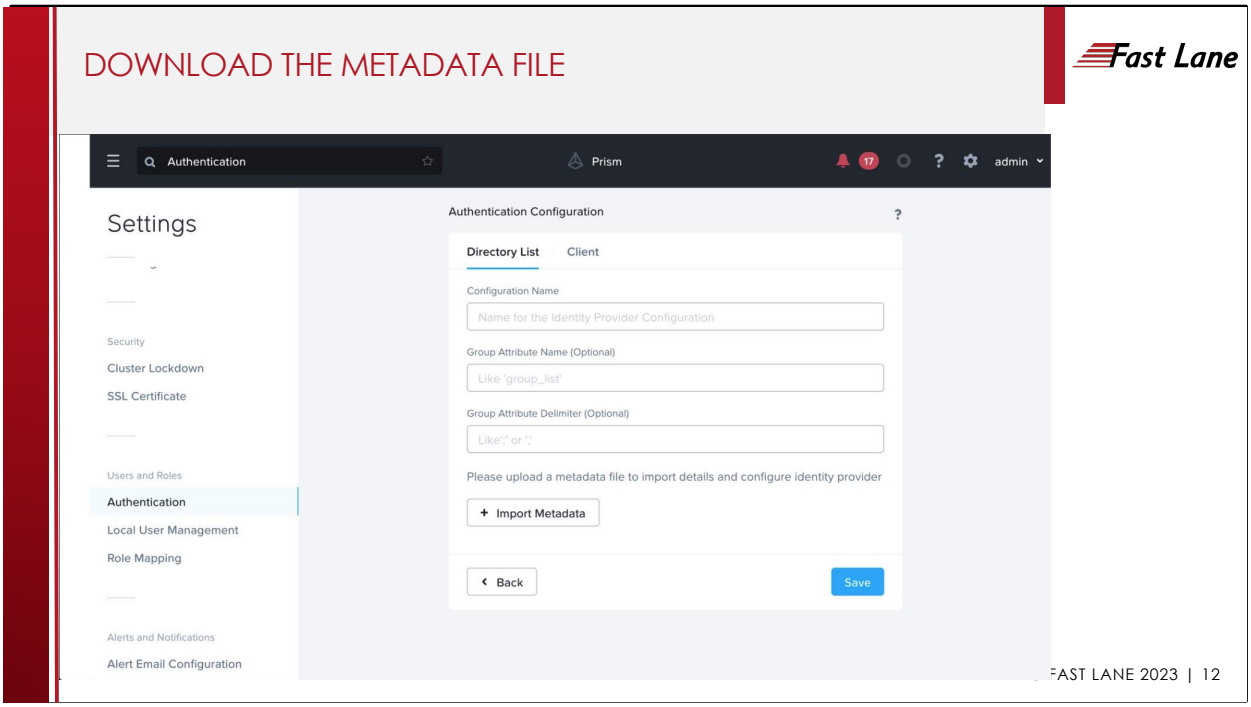
Net zoals het toevoegen van een authenticatiemap, wordt ook een op SAML gebaseerde identiteitsprovider toegevoegd vanuit de categorie Gebruiker en rollen van het menu Instellingen in Prism Central. Klik in het dialoogvenster Verificatieconfiguratie op de knop + Nieuwe IDP.



Configuring an IDP

Om een IDP te configureren, moet u een configuratienaam, een optionele groepskenmerknaam, een optioneel groepskenmerkscheidingsteken opgeven en het metagegevensbestand uploaden dat de informatie van de identiteitsprovider bevat. Dit metadatabestand is meestal een XML-bestand dat wordt verkregen via de website van de identiteitsprovider, dat kan worden gedownload en vervolgens kan worden geüpload naar Prism Central.

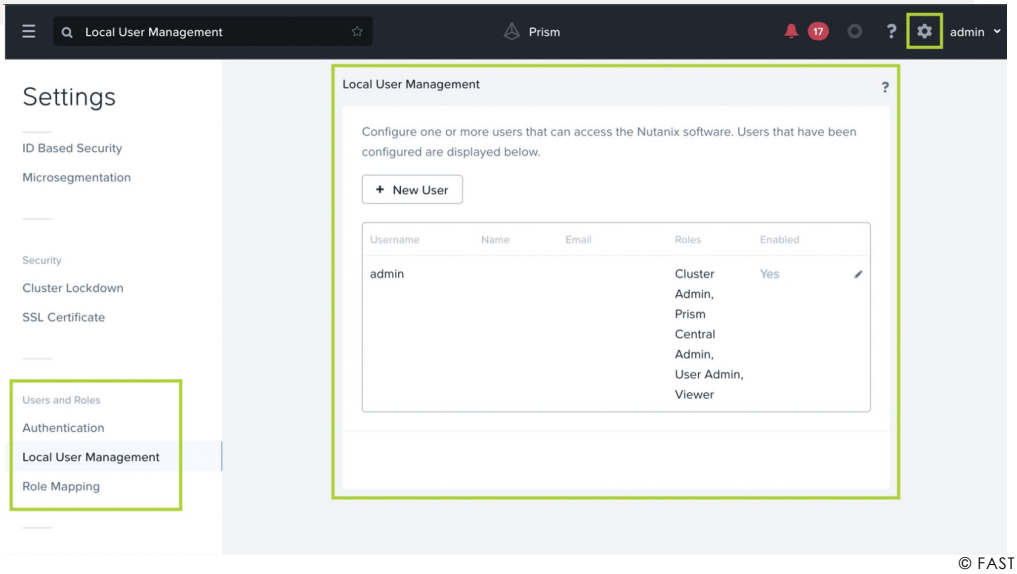
Hiermee voltooit u de IDP-configuratie in Prism Central, maar u moet ook de callback-URL voor Prism Central configureren op de identiteitsprovider. Om dit te doen, moet u een metagegevensbestand downloaden dat Prism Central beschrijft vanuit het dialoogvenster Authenticatieconfiguratie en vervolgens het XML-bestand uploaden naar de identiteitsprovider.



Downloading the Metadata File

En wanneer u het metadatabestand met Prism Central-informatie moet downloaden om de callback-URL te configureren, kunt u dit doen vanuit het dialoogvenster Configuring Authentication, zoals aangegeven in de volgende afbeelding.

LOCAL USERS



Any user accounts that you create can have their name, email, password, language, and roles updated at any time. Custom user accounts can also be deleted after creation.

The default 'admin' user cannot be deleted and the roles associated with this account cannot be changed. However, some information - first and last name, email, password, and language - can still be updated or modified.

The roles that the admin account has access to are:

•User Administrator, which allows the user to view information, perform any administrative task, and create or modify user accounts. This role grants full permissions.

•Cluster Administrator, which allows the user to view information and perform any administrative task except create or modify user accounts.

•Backup Admin, which allows the users to perform backup related administrative tasks. This role does not have permission to perform cluster or user tasks.

The User Admin and Cluster Admin roles can also be assigned to custom local user accounts that are created in Prism Central. If no role is assigned to a local user account, that account will be granted view only rights.

CREATE A LOCAL USER

Fast Lane

- User data like name, email, password etc can update any time
- The default admin user cannot be deleted

Any user accounts that you create can have their name, email, password, language, and roles updated at any time. Custom user accounts can also be deleted after creation.

The default 'admin' user cannot be deleted and the roles associated with this account cannot be changed. However, some information - first and last name, email, password, and language - can still be updated or modified.

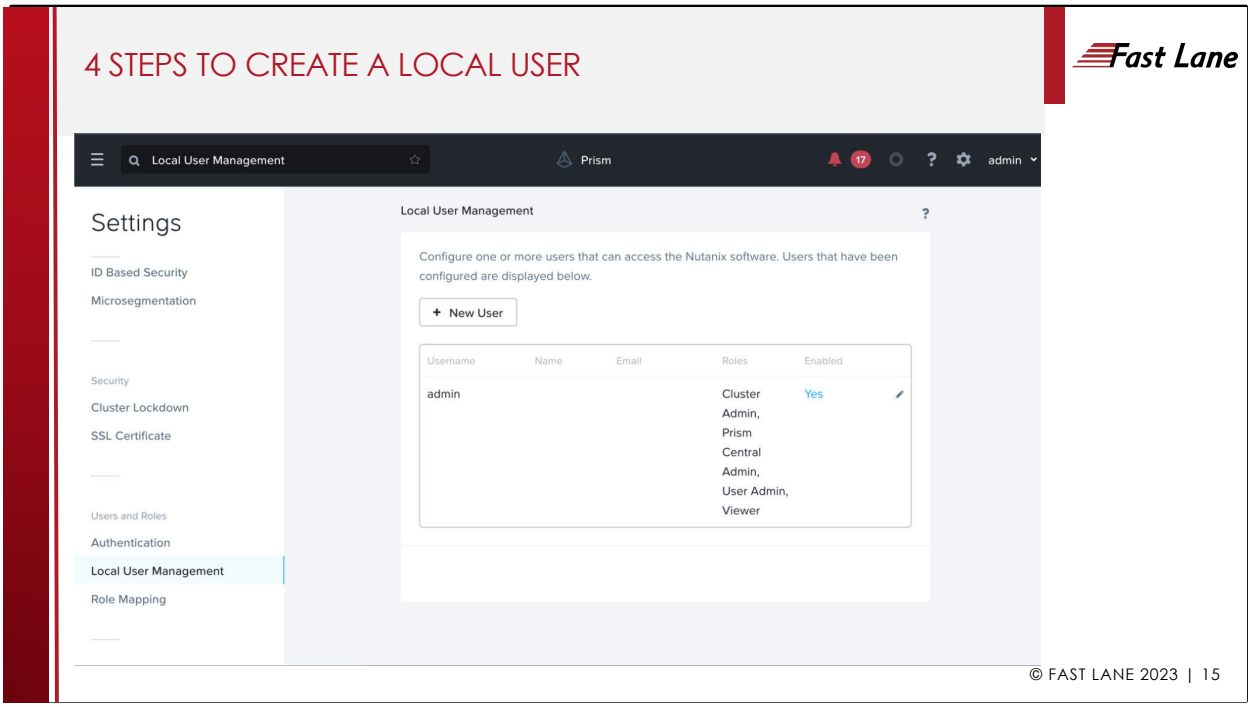
The roles that the admin account has access to are:

•User Administrator, which allows the user to view information, perform any administrative task, and create or modify user accounts. This role grants full permissions.

•Cluster Administrator, which allows the user to view information and perform any administrative task except create or modify user accounts.

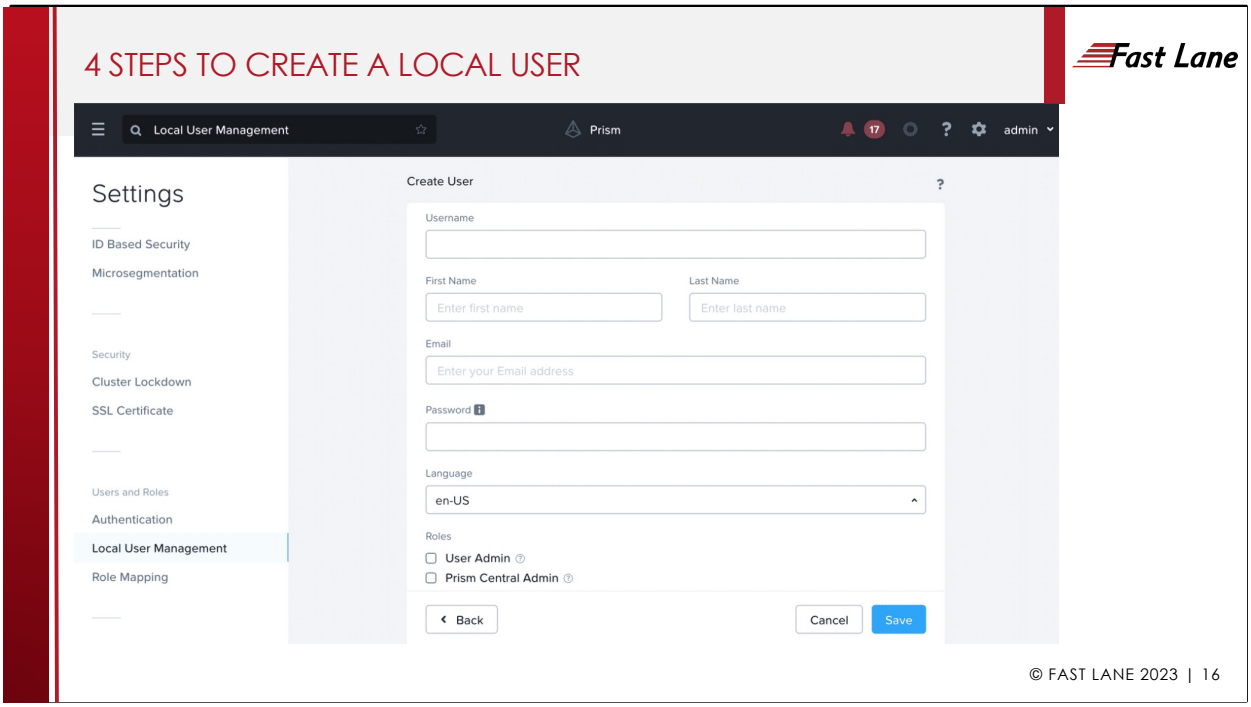
•Backup Admin, which allows the users to perform backup related administrative tasks. This role does not have permission to perform cluster or user tasks.

The User Admin and Cluster Admin roles can also be assigned to custom local user accounts that are created in Prism Central. If no role is assigned to a local user account, that account will be granted view only rights.



Step 1

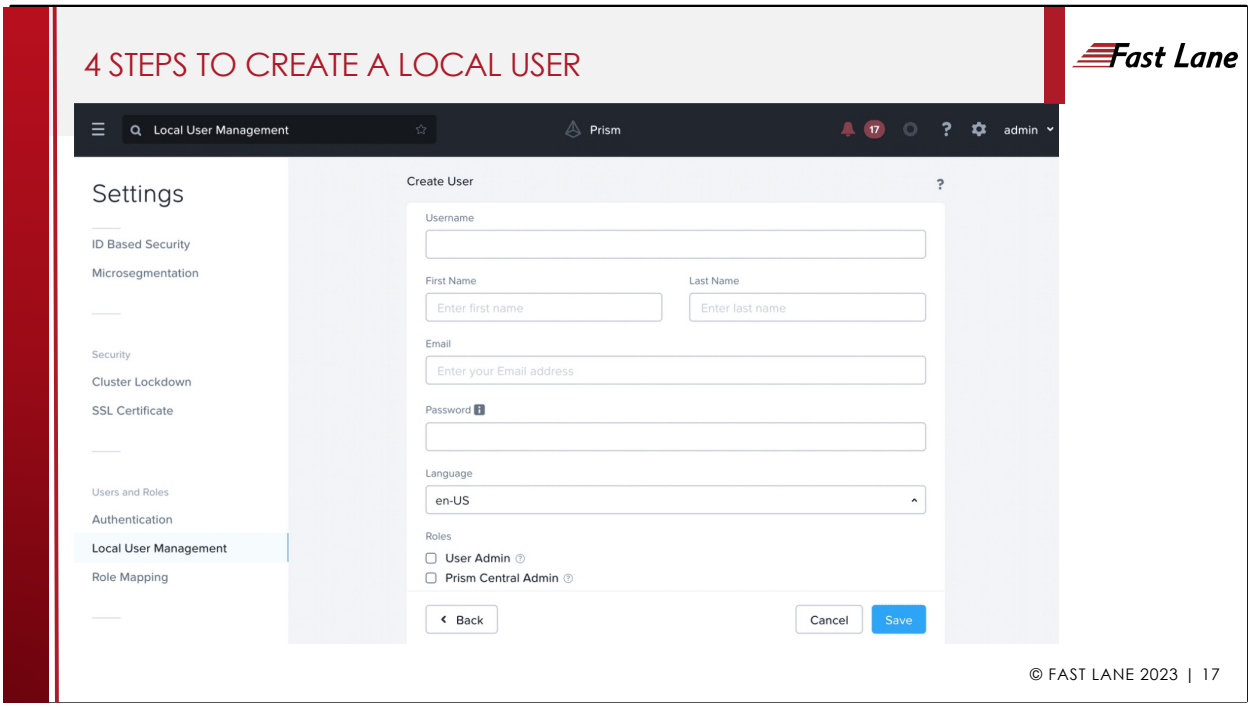
Als u een lokaal gebruikersaccount wilt maken in Prism Central, gaat u naar de pagina Instellingen, scrolt u omlaag naar de categorie Gebruikers en rollen en klikt u op Lokaal gebruikersbeheer. Wanneer u op + Nieuwe gebruiker klikt, krijgt u het dialoogvenster te zien dat wordt weergegeven in de volgende afbeelding.



Step 2

Als u een nieuwe gebruiker wilt maken, moet u een gebruikersnaam, voornaam, achternaam en wachtwoord opgeven en een taal selecteren (Engels, Vereenvoudigd Chinees, Japans en Koreaans).

Opmerking: bij het maken van een gebruikersnaam zijn slechts enkele soorten speciale tekens toegestaan
toegestaan, zoals streepjes of underscores. Daarom zijn john-smith en john_smith geldige gebruikersnamen, maar john.smith niet. Als u een ongeldig speciaal teken in een gebruikersnaam gebruikt, wordt u gevraagd dit te wijzigen.

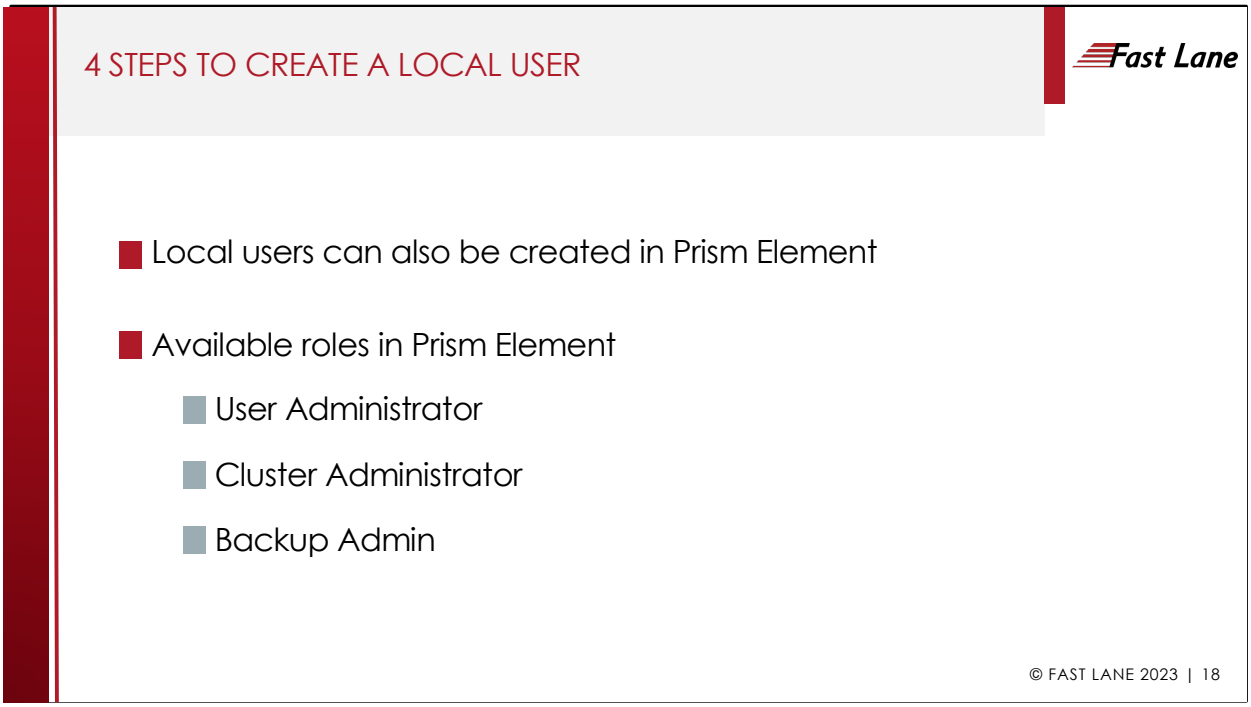


Step 3

Zoals we eerder hebben besproken, zijn er twee rollen beschikbaar voor toewijzing.

Door een account de rol van gebruikerbeheerder toe te wijzen, kan die gebruiker informatie in Prism Central bekijken, administratieve taken uitvoeren en gebruikersaccounts maken en wijzigen.
Door een account de rol van Prism Central-beheerder toe te wijzen, kan die gebruiker informatie in Prism Central bekijken en alle administratieve taken uitvoeren. Een Prism Central-beheerder kan echter geen gebruikersaccounts maken en wijzigen.

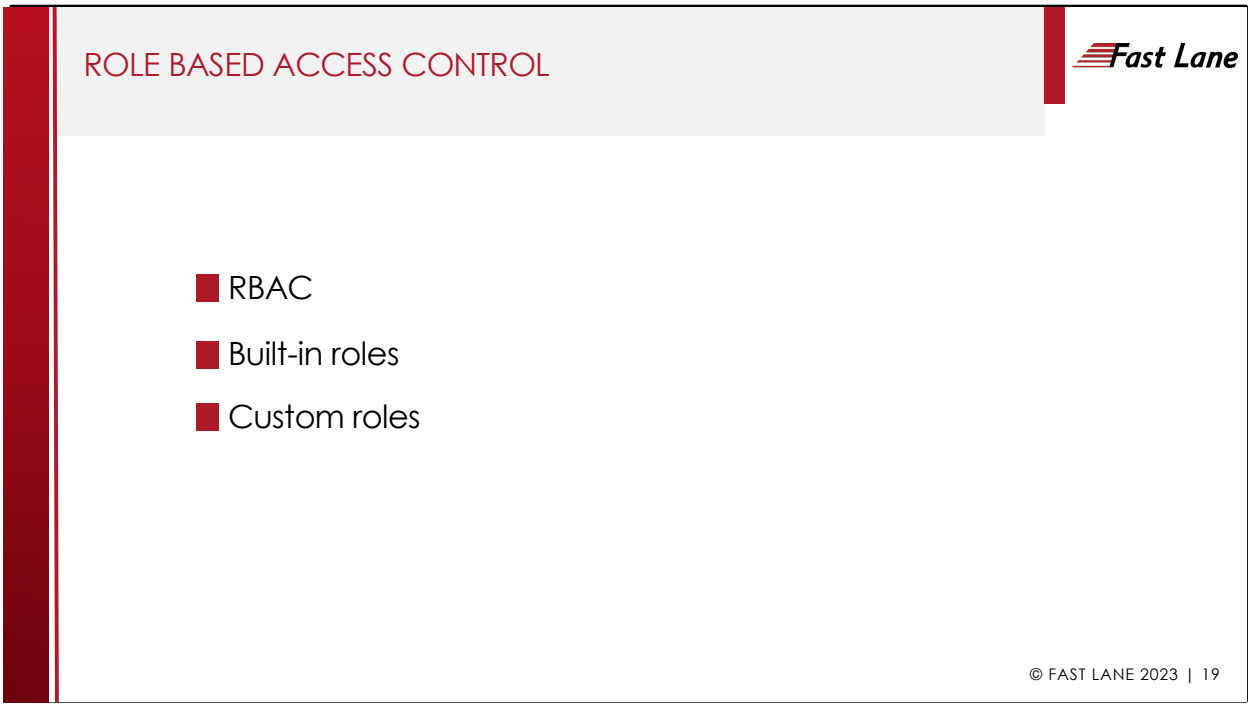
Het is ook mogelijk om helemaal geen rol toe te wijzen aan een gebruikersaccount. In dit geval (dat wil zeggen, als zowel de gebruikersbeheerder als de Prism Central-beheerdersopties niet zijn aangevinkt), kan de gebruiker inloggen en informatie bekijken in Prism Central, maar kan hij geen administratieve taken uitvoeren of gebruikersaccounts beheren.



Step 4

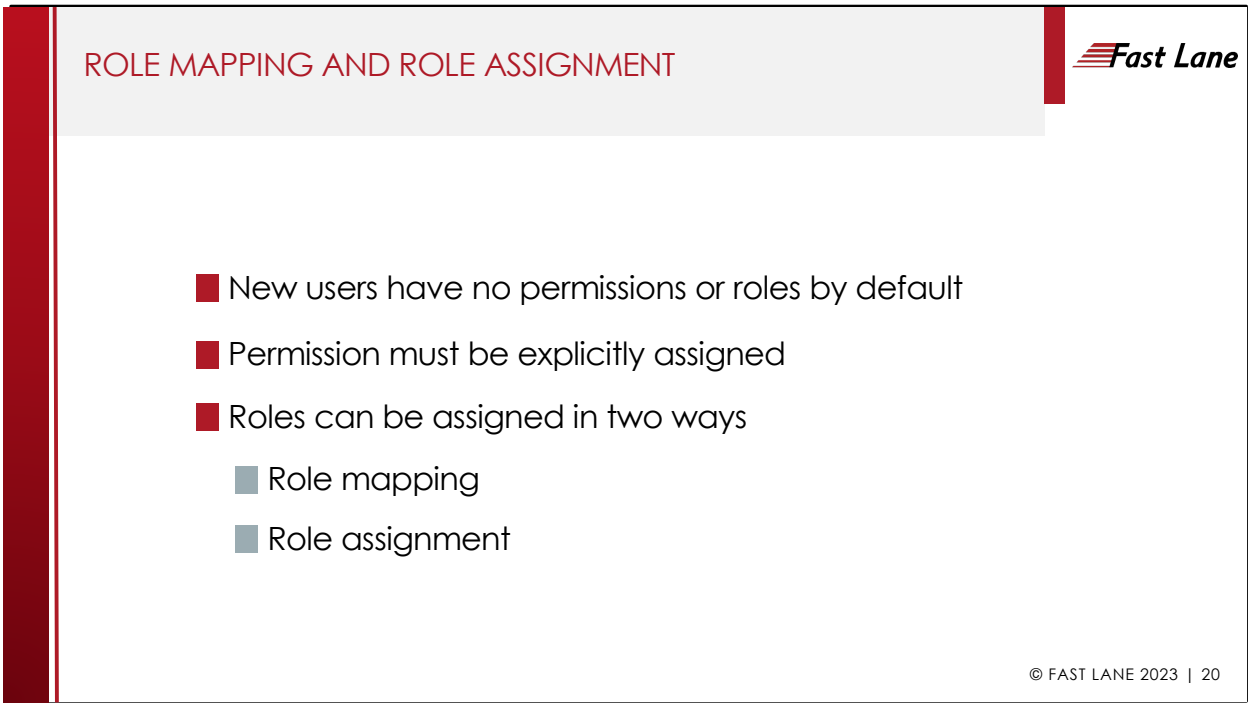
Lokale gebruikersaccounts kunnen ook worden aangemaakt in Prism Element. De procedure is hetzelfde (Instellingen > Gebruikers en rollen > Lokaal gebruikersbeheer > + Nieuwe gebruiker) en u wordt gevraagd om dezelfde informatie op te geven die vereist is bij het aanmaken van een nieuwe lokale gebruiker in Prism Central.

De beschikbare rollen in Prism Element zijn echter Gebruikersbeheerder, Clusterbeheerder en Back-upbeheerder. Voor stapsgewijze instructies voor het maken van gebruikersaccounts in Prism Central, zie Een gebruikersaccount maken (opent in een nieuw tabblad) in de beveiligingshandleiding op de Nutanix Support Portal.



Met rolgebaseerde toegangscontrole (RBAC) in Prism Central kunt u zowel ingebouwde als aangepaste rollen gebruiken om machtigingen op een gedetailleerd niveau te definiëren en deze rollen vervolgens aan gebruikers toe te wijzen.

Standaard zijn er tien ingebouwde rollen beschikbaar in Prism Central.
Zij zijn:
Super Admin, Self-Service Admin, Prism Admin, Project Admin, VPC Admin, Network Infra Admin, Prism Viewer, Operator, Developer en Consumer.



Nadat u authenticatie hebt geconfigureerd, krijgen gebruikers en directory's niet standaard machtigingen of rollen toegewezen. Machtigingen moeten expliciet worden toegewezen aan gebruikers, geautoriseerde directory's of organisatie-eenheden.

Er zijn twee manieren waarop u rollen kunt toewijzen aan gebruikers of groepen gebruikers: Roltoewijzing en Roltoewijzing.

Met Role Mapping kunt u vooraf gedefinieerde rollen gebruiken in Prism Central - User Admin, Cluster Admin en Viewer - en deze rollen toewijzen aan gebruikers, groepen en organisatie-eenheden. Deze functie is toegankelijk via het menu Instellingen in de categorie Gebruikers en rollen. Klik op Rollentoewijzing om nieuwe toewijzingen te maken of bestaande te wijzigen of te verwijderen.

Rollentoewijzing wordt doorgaans gebruikt om basisrollentoewijzingen te maken. Als u aangepaste rollen gebruikt in Prism Central, kunt u die rollen toewijzen aan gebruikers of groepen met de functie Roltoewijzing. Selecteer hiervoor een rol op het rollendashboard, klik op de vervolgkeuzelijst Acties en selecteer Roltoewijzing.

Op de pagina Roltoewijzing kunt u gebruikers, gebruikersgroepen of organisatie-eenheden selecteren waarop de geselecteerde rol wordt toegepast. Daarnaast kunt u ook entiteiten selecteren. De lijst met beschikbare entiteiten hangt af van de rol die momenteel wordt toegewezen. In de volgende afbeelding zijn bijvoorbeeld, aangezien er een aangepaste VM-beheerdersrol is geselecteerd, de entiteiten waaraan deze kan worden toegewezen allemaal gerelateerd aan VM's - AHV VM's, clusters, subnetten of alle selecteerbare entiteitstypen.

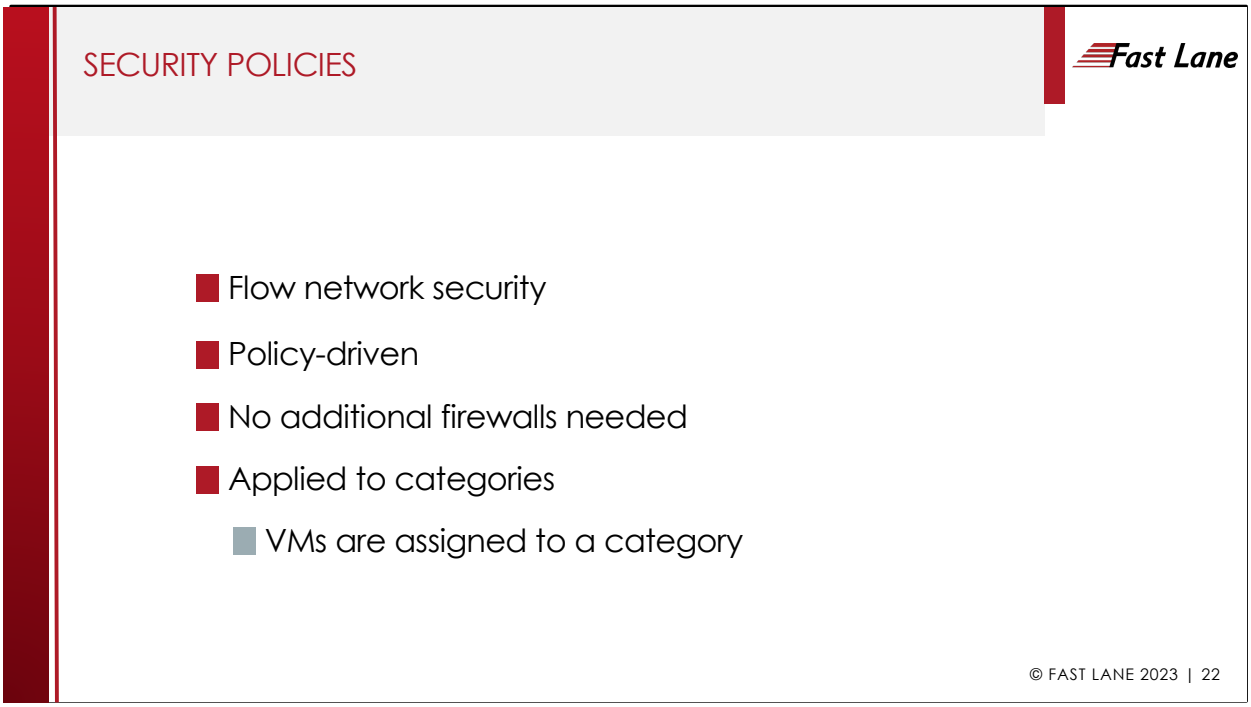
CLUSTER LOCKDOWN

Fast Lane

- Disable password authentication
- Enforce keybased SSH access to the CVM
- Only default nutanix and admin accounts have access

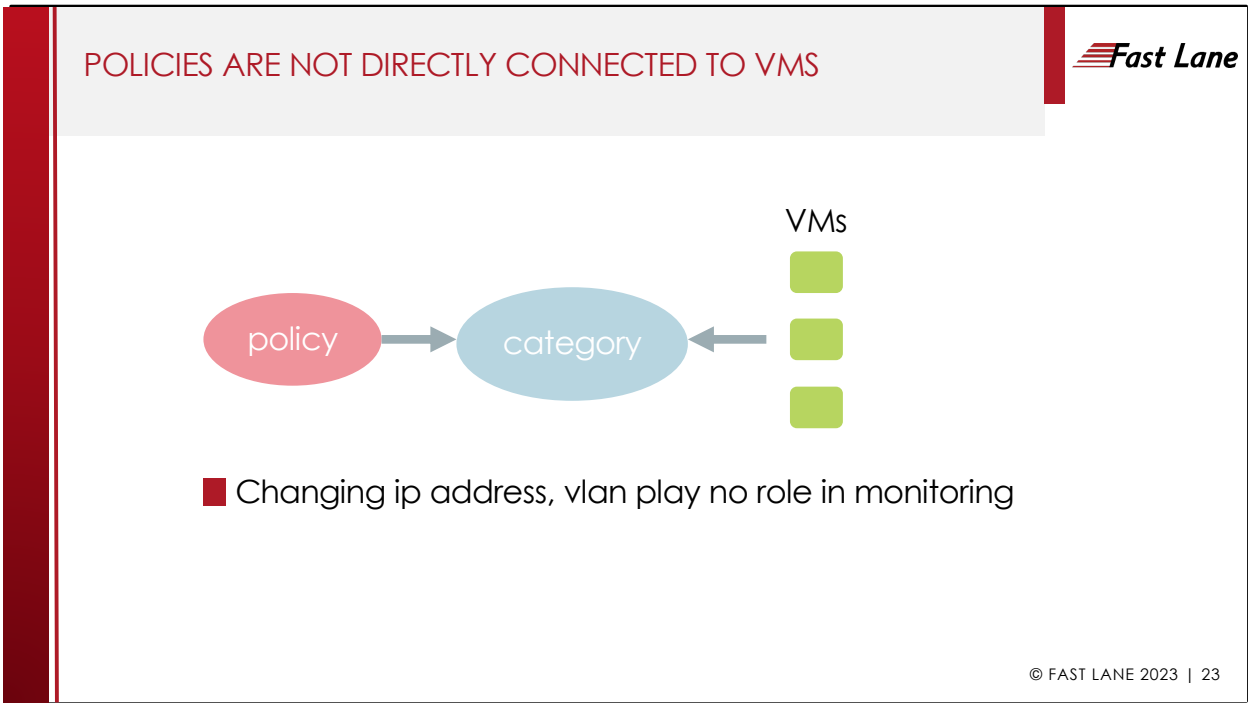
Clustervergrendeling kan worden gebruikt om op wachtwoord gebaseerde authenticatie uit te schakelen en op sleutel gebaseerde SSH-toegang af te dwingen tot de controller-VM en de host die zijn vergrendeld. Alleen de standaard 'nutanix'- en 'admin'-accounts kunnen worden gebruikt om toegang te krijgen tot een CVM of host die is vergrendeld.

U kunt een of meer sleutelparen maken en de openbare sleutels toevoegen om op sleutels gebaseerde SSH-toegang mogelijk te maken. Als de beveiligingsvereisten van de site dit echter niet toestaan, kunt u alle openbare sleutels verwijderen om SSH-toegang te voorkomen.



Nutanix biedt Flow Netwerkbeveiliging. Flow maakt gebruik van een beleidsgestuurd beveiligingsraamwerk dat verkeer inspecteert dat binnen het datacenter komt en eindigt, waardoor er geen extra firewalls nodig zijn.

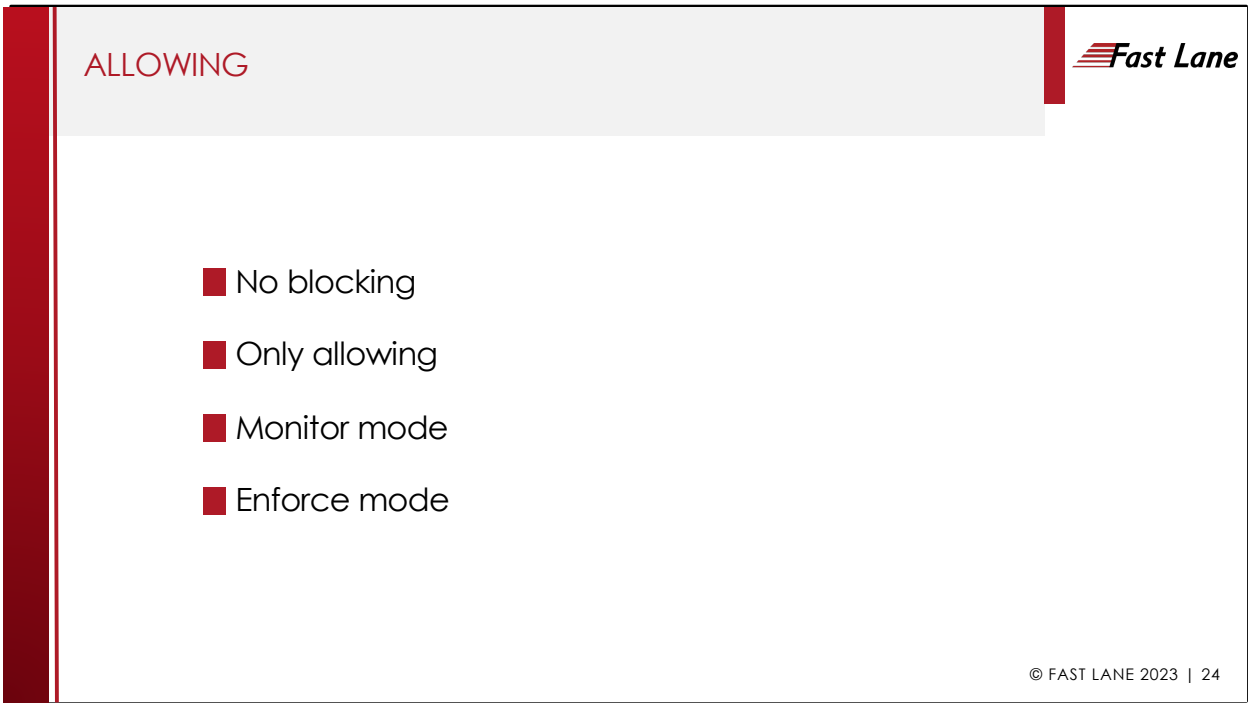
Aangezien VM's worden toegewezen aan een categorie en een beleid wordt toegepast op een categorie, is beveiligingsbeleid niet rechtstreeks verbonden met VM's.



Zoals we enkele ogenblikken eerder hebben geleerd, worden entiteiten binnen een Flow-beveiligingsbeleid geïdentificeerd aan de hand van de categorieën waartoe ze behoren. Nadat een VM is gekoppeld aan een categorie en die categorie is gekoppeld aan een beleid, blijft het verkeer worden gecontroleerd, zelfs als de VM naar een ander netwerk migreert of het IP-adres wijzigt. Netwerkattributen, zoals IP-adres en VLAN, spelen geen rol bij verkeersmonitoring.

Dit is mogelijk omdat het beveiligingsbeleid van Flow toepassingsgerichte beleidstaal gebruikt. Dit betekent simpelweg dat u eerst de VM's moet specificeren die horen bij de applicatie die u wilt beschermen, en vervolgens de netwerken of entiteiten moet identificeren waarmee u die VM's wilt laten communiceren (zowel inkomende als uitgaande richtingen).

Meer gedetailleerd beleid kan worden gedefinieerd door ook te specificeren welke poorten en protocollen kunnen worden gebruikt voor communicatie.



Het is echter belangrijk op te merken dat u geen categorieën en subnetten kunt specificeren die u wilt blokkeren. Dit komt omdat het aantal van deze entiteiten doorgaans veel groter is dan de lijst met toegestane entiteiten, en de neiging heeft om ook veel sneller te groeien. In plaats daarvan wordt al het andere geblokkeerd zodra u specificeert welke categorieën en subnetten mogen communiceren. Dit resulteert in een kleinere, strakkere beleidsconfiguratie die gemakkelijker kan worden gewijzigd, gecontroleerd en gecontroleerd.

Beleid kan ook op twee manieren worden afgedwongen. Een beleid kan worden ingesteld om te worden uitgevoerd in de monitormodus, waardoor al het verkeer is toegestaan, inclusief verkeer dat niet is toegestaan door het beleid. Zo krijgt u een beter inzicht in de impact van het beleid en kunt u deze indien nodig verder verfijnen. Zodra een beleid en de impact ervan zijn bepaald, kunt u het overschakelen naar de modus Afdwingen, waardoor het beleid effectief wordt ingeschakeld en al het verkeer wordt geblokkeerd dat niet is toegestaan door de configuratie.

TYPES OF SECURITY POLICIES

Fast Lane

- Application security policy
- Isolation environment policy
- Quarantine policy
- Vdi policy

Toepassingsbeveiligingsbeleid
–
Met een toepassingsbeveiligingsbeleid kunt u (zoals eerder beschreven) categorieën van VM's selecteren, toegestane verkeersbronnen en bestemmingen specificeren en uw beleid alleen toepassen op die entiteiten. Al het andere verkeer wordt geblokkeerd.

Isolatie Milieubeleid
–
Met een isolatie-omgevingsbeleid kunt u al het verkeer tussen twee groepen VM's blokkeren. U wilt bijvoorbeeld dat al uw productie-VM's niet kunnen communiceren met uw Dev/Test- of Sandbox-VM's. Als u in dit scenario twee categorieën heeft (één voor productie en één voor sandbox), kunt u een beleid definiëren dat voorkomt dat VM's in die twee groepen met elkaar communiceren. Communicatie tussen VM's binnen een categorie is echter nog steeds toegestaan. Alle VM's binnen de productiecategorie kunnen dus nog steeds met elkaar communiceren. Evenzo zullen alle VM's binnen de Sandbox-categorie ook met elkaar kunnen communiceren.

Quarantainebeleid

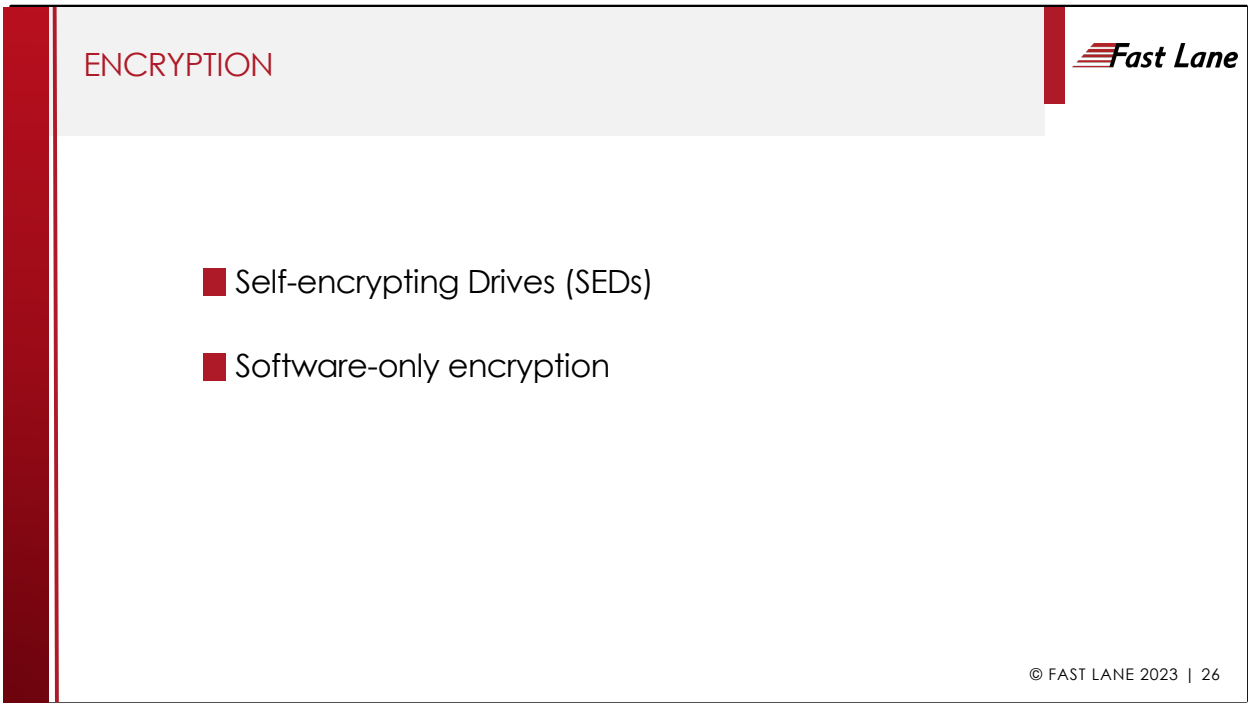
–

Een quarantainebeleid, zoals de naam al doet vermoeden, is bedoeld om te worden gebruikt wanneer u een geïnfecteerde VM wilt isoleren.

VDI-beleid

–

Een VDI-beleid kan worden gebruikt om een VDI-omgeving te beveiligen en stelt u in staat beveiligingsbeleid te maken op basis van gebruikers en groepen in een Active Directory-domein. Wanneer gebruikers inloggen op hun virtuele desktops, plaatst de ID-firewall van Flow VM's automatisch in bepaalde vooraf gedefinieerde categorieën, zodat het beveiligingsbeleid automatisch wordt afgedwongen.



Nutanix biedt twee opties die u kunt gebruiken om uw gegevens te beveiligen:

DARE met behulp van Self-Encrypting Drives (SED's). Dit omvat het gebruik van een combinatie van SED's en een externe Key Management Server (KMS) om gegevens te beveiligen terwijl deze in rust zijn.

DARE met behulp van software-encryptie. Als versleuteling met alleen software is ingeschakeld, gebruikt AOS de versleutelingsstandaard AES-256 om uw gegevens te versleutelen. U kunt de Nutanix Native Key Manager (zowel lokaal als extern) of een externe KMS gebruiken om uw sleutels te beveiligen.

Fast Lane

8 Steps to work with SEDs

Step 1
–
SED's worden geïnstalleerd voor alle gegevensstations in een cluster. Deze schijven zijn FIPS 140-2 gevalideerd en gebruiken FIPS 140-2 gevalideerde cryptografische modules. Dit is eenvoudig te doen voor een gloednieuw cluster. Een bestaand cluster kan worden geconverteerd door bestaande schijven te vervangen door SED's.
Stap 2
–
Gegevens op de schijven zijn gecodeerd, maar lees- en schrijftoegang is open. Standaard wordt de ingebouwde fabrikantsleutel gebruikt om de toegang tot gegevens te beschermen. Wanneer gegevensbescherming voor het cluster echter is ingeschakeld, moet de CVM een juiste sleutel leveren.
Stap 3
–
Een symmetrische gegevenscoderingssleutel (DEK), zoals AES 256, wordt toegepast op alle gegevens die worden geschreven of gelezen. De sleutel is alleen bekend bij de schijfcontroller en verlaat nooit het fysieke subsysteem, dus er is geen manier om rechtstreeks vanaf de schijf zelf toegang te krijgen tot de gegevens.
Stap 4

–
Een andere sleutel, bekend als een sleutelversleutelingssleutel (KEK), wordt gebruikt om de DEK te versleutelen/ontsleutelen en zich te authenticeren bij de schijf. U hebt misschien gehoord dat dit door andere leveranciers een authenticatiesleutel of pincode wordt genoemd. Elke schijf heeft een afzonderlijke KEK, gegenereerd door de FIPS-compatibele generator voor willekeurige getallen in de schijfcontroller. Hoewel de KEK op het knooppunt wordt gegenereerd, wordt deze niet lokaal opgeslagen; alle KEK's worden naar de KMS gestuurd voor veilige opslag en ophalen.
Stap 5
–
Een leidercoderingssleutel (MEK) wordt gebruikt om KEK's te coderen.
Stap 6
–
Sleutels worden opgeslagen in een KMS die los staat van het cluster. Elk knooppunt onderhoudt een set certificaten en sleutels om een veilige verbinding met de KMS tot stand te brengen. De CVM communiceert met de sleutelbeheerserver via het Key Management Interoperability Protocol (KMIP) om schijfsleutels te uploaden en op te halen.
Stap 7
–

Hoewel er slechts één KMS vereist is, worden meerdere apparaten aanbevolen, zodat de KMS geen single point of failure wordt. KMSes moeten in geclusterde modus worden geconfigureerd, zodat ze aan het Nutanix-cluster kunnen worden toegevoegd als een enkele, veerkrachtige entiteit die bestand is tegen een enkele storing.
Stap 8
–
Wanneer een knooppunt volledig wordt uitgeschakeld en vervolgens weer wordt ingeschakeld, haalt de CVM de stationssleutels op van de KMS en gebruikt deze om de stations te ontgrendelen.

SUMMARY

Fast Lane

- Security is built from the ground up
- STIG SCMA and SAML can be used
- Local Accounts
- Cluster Lockdown
- Encryption at rest

In this module, you learned:
•How security is built into the Nutanix platform from the ground up.
•How STIGs and SCMA are used and automated to self-heal a cluster using security baselines.
•How to configure authentication in Prism Central via a directory service or a SAML-based identity provider.
•How to enable and configure client (that is, two-way) authentication.
•How to create and manage local user accounts in Prism Central.
•What role-based access control is, how it works, and how you can use both built-in and custom roles to assign permissions to your users.
•What cluster lockdown is.
•What Flow Network Security is, how security polices work, and what types of security policies are available.
•How Nutanix implements both hardware and software-based data-at-rest encryption.